Универзитет у Београду
Математички факултет

Милица Б. Анђелић

ПРСТЕНИ КОСИХ ПОЛИНОМА

Магистарски рад

Комисија
1. Ž. Mijajlović
2. G. Kalajdžić
3. A. Lipkovski
4. M. Rašković
5. D. Tošić

Београд, 2004.

Садржај

ПРЕДГОВОР

Најадекватније уопштење појма прстена полинома у некомутативној алгебри био би појам слободне алгебре, или општије појам тензорског прстена. Међутим, постоји и једно "половично" уопштење, а то су прстени косих полинома. Овај појам настао је у теорији диференцијалних једначина. Наиме за $f' = df/dx$ прстен линеарних диференцијалних оператора може се видети и као прстен косих полинома $k(x)[D; 1, \prime]$. У овом облику прстен косих полинома јавио се у радовима Шлесингера још 1897. године. Прву апстрактну студију о овој класи некомутативних прстена дао је Оре 1932. године. Од тада прстени косих полинома предмет су проучавања многих алгебриста и то све до данашњих дана. Последњих година најзначајније резултате дали су Кон, Лем, Лирој и Анин. Овај рад управо представља синтезу како старих тако и нових резултата везаних за ову класу некомутативних прстена.

У првој глави овог рада дат је приказ основних појмова некомутативне алгебре који су значајни за материју изложену у наставку. Овде је, пре свега, дат приказ основних примера некомутативних прстена и то почев од Хамилтоновог прстена реалних кватерниона. Конструкцијом овог прстена Хамилтон је 1843. дао први пример некомутативног прстена. У наставку је изложена важна конструкција тела разломака Ореовог домена, а затим дефиниција једнозначне факторизације у некомутативним прстенима. Даље, је приказан алгоритам за редукцију матрица над главноидеалским прстенима, као и његова примена на опис коначно генерисаних модула над главноидеалским прстенима. Најзад, у овој глави показана су основна својства тела, као специјалне класе некомутативних прстена. Посебно је на примеру косих Лоранових редова показано да уређено тело не мора бити комутативно, уколико уређење није архимедовско. Такође су предочени и неки геометријски аспекти теорије тела и с тим у вези Папусова теорема као занимљив еквивалент закона комутативности у афиној геометрији.

У другој глави детаљно је уведен појам прстена косих полинома, издвојене су основне особине, основни примери као и опис структуре идеала ових прстена. Даље је изложена конструкција прстена косих степених редова комплетирањем прстена косих полинома. Затим следи Мальцев-Нојманова конструкција по којој се свака групна алгебра тотално уређене групе може утопити у тело. Овај резултат доказали су, независно један од другог, Мальцев 1948. и Нојман 1949. године. Затим је уведен појам J-прстена, које је први конструисао Јатегаонакар 1969. и то

коришћењем трансфинитне индукције. Затегаонакар је овом конструкцијом дао пример левог Нетериног прстена за чији Џејкобсонов радикал $\mathcal{J}$ важи $\cap\mathcal{J}^n \neq 0$, и у ком постоје елементи са бесконачном факторизацијом. Последњи део друге главе посвећен је псеудо-линеарним трансформацијама, уопштењу појма линеарних пресликавања. Изведена је њихова матрична репрезентација, и показано да у општем случају за ову класу пресликавања не важи Кејли-Хамилтонова теорема.

Аналогно као и у комутативном случају у трећој глави уведен је појам раширења тела као и Галуаовог раширења. Посебно су разматрани поједини типови једначина над телима, као и особине нула полинома над телима. Остатак главе посвећен је специјалним случајевима: квадратним, псеудолинеарним и спољашњим цикличним Галуаовим раширењима.

Четврта глава представља синтезу претходних преточену у једну примену прстена косих полинома. Примена се односи на одређивање критеријума инвертибилности уопштене Вандермондове матрице. Такође је уведен и појам детерминанте над телом - Диодонеове детерминанте.

Овај рад непосредно је инспирисан програмом семинара Некомутативна алгебра Математичког факултета у Београду. Поједини делови рада, посебно прва и друга глава, у непосредној су вези са темама обрађеним на семинару. Рад је настао под менторством проф. др. Гојка Калајџића, коме дугујем посебну захвалност за упућивање у ову област, као и за бројне корисне примедбе упућене током израде овог рада.

Београд,
децембра 2003.

Милица Анђелић

1

УВОДНО ПОГЛАВЉЕ

1.1 Основни појмови о некомутативним прстенима и телима

На почетку дајемо кратак преглед основних термина и ставова теорије прстена са посебним нагласком на њеним некомутативним аспектима.

Прстеном ћемо звати прстен са јединицом који није обавезно комутативан. *Леви (десни) идеал* прстена R је његов подскуп затворен за сабирање и множење слева (здесна) елементима из R; I је *идеал* у R уколико је и леви и десни идеал. Прстен R је *прост* ако су (0) и R једини идеали у њему, то јест за сваки елемент $a \in R \setminus \{0\}$ идеал генерисан са a је R. Отуда је прстен R прост акко за свако $a \neq 0$ у R постоји једнакост $\sum b_i a c_i = 1$ за одговарајуће $b_i, c_i \in R$.

Елемент $a \in R \setminus \{0\}$ је *леви (десни) делитељ нуле* ако постоји елемент $b \in R \setminus \{0\}$ такав да је $ab = 0$ ($ba = 0$). За разлику од комутативних прстена, у некомутативним, леви делитељ нуле не мора бити и десни и обратно, што ће потврдити и следећи пример.

Пример 1. Нека је $R = \left\{ \begin{bmatrix} x & y \\ 0 & z \end{bmatrix} | x, z \in \mathbb{Z}, y \in \mathbb{Z}/2\mathbb{Z} \right\}$; R је прстен у односу на сабирање и множење матрица. За $A = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, важи $AB = 0$, па је A леви делитељ нуле, али није и десни, с обзиром на то да је једнакост

$$0 = \begin{bmatrix} x & y \\ 0 & z \end{bmatrix} \cdot \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 2x & y \\ 0 & z \end{bmatrix}$$

задовољена само за $\begin{bmatrix} x & y \\ 0 & z \end{bmatrix} = 0$. С друге стране је $B^2 = 0$, па је B и леви и десни делитељ нуле. ∇

Прстен R је *домен* ако $ab = 0$ повлачи $a = 0$ или $b = 0$, тако да у доменима немамо делитеља нуле (ни левих ни десних).

Елемент $a \in R$ је *десно инвертибилан* ако постоји $b \in R$ који ћемо звати *десним инверзом* од a за који је $ab = 1$. Аналогно за леву инвертибилност

и леви инверз. Ако a има и леви и десни инверз онда су они једнаки. У том случају кажемо да је a *инвертибилан* или *јединичан*. Скуп свих инвертибилних елемената прстена R означаваћемо са $R^\times$. Овај скуп је група у односу на множење у R.

У одређеном смислу најидеалнији објекти у некомутативној теорији прстена су *тела* - прстени у којима су сви елементи осим нуле инвертибилни. У пракси довољно је проверити да је сваки $a \neq 0$ у R десно инвертибилан, то јест прстен R је тело акко су му једини десни идеали (0) и R.

Уопште, сваки резултат "здесна" важи и "слева" што показујемо применом истих аргумената само с друге стране. У вези са тим дефинишемо и прстен R^{op} - *опозит* прстена R са елементима a^{op} који су у $1-1$ коресподенцији са елементима a из R и множењем дефинисаним са

$$a^{op} \cdot b^{op} = (ba)^{op}, \quad a, b \in R.$$

Практично, ако неко тврђење важи здесна, онда аналогно тврђење важи и слева применом истог на опозит прстена R.

Даље, наводимо примере некомутативних прстена и кроз њих указујемо на нека њихова својства по којима се ови прстени битно разликују од комутативних.

Пример 2. *Хамилтонов прстен реалних кватерниона*
Реални кватерниони $\mathbb{H}$ су једна четвородимензиона $\mathbb{R}$-алгебра са базом $1, i, j, k$ тј.

$$\mathbb{H} = \mathbb{R}1 \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$$

и множењем задатим са

$$i^2 = -1, \quad j^2 = -1, \quad ij = -ji = k.$$

За $\alpha = a + bi + cj + dk \in \mathbb{H}$ дефинишемо $\overline{\alpha} = a - bi - cj - dk$. Тада је $\alpha\overline{\alpha} = \overline{\alpha}\alpha = a^2 + b^2 + c^2 + d^2 \in \mathbb{R}$. То јест ако је $\alpha \neq 0$, онда $\alpha \in \mathbb{H}^\times$, па је $(\mathbb{H}, +, \cdot)$ тело. Претходно важи и ако $\mathbb{R}$ заменимо произвољним пољем у којем

$$(a, b, c, d) \neq 0 \Rightarrow a^2 + b^2 + c^2 + d^2 \neq 0.$$

∇

Пример 3. *Слободни k-прстени*
Нека је k прстен и $(x_i | i \in I)$ систем независних неодређених над k, које не комутирају. Слободан прстен генерисан са $(x_i | i \in I)$, који ћемо означавати са $R = k\langle x_i | i \in I\rangle$, има за елементе полиноме по x_i са коефицијентима у k. Придев слободан односи се на универзално својство прстена R, да се сваки хомоморфизам прстена $\varphi_0 : k \to k'$ за сваки скуп $\{a_i | i \in I\} \subseteq k'$ са својством да сваки a_i комутира са сваким елементом из $\varphi_0(k)$, може на јединствен начин продужити до хомоморфизма $\varphi : R \to k'$, за који је $\varphi|_k = \varphi_0$ и $\varphi(x_i) = a_i$ за свако $i \in I$. Слободан k-прстен $k\langle x_i | i \in I\rangle$ има битно различита својства од прстена полинома $k[x_i | i \in I]$ у коме неодређене комутирају. Примера ради, у слободном k-прстену $k\langle x, y\rangle$ потпрстен генерисан скупом $\{z_i = xy^i | 0 \leqslant i \leqslant n\}$ је слободан k-прстен са $n+1$ генератором. Отуда $k\langle x, y\rangle$ садржи изоморфне копије $k\langle x_0, \ldots, x_n\rangle$ за свако $n \in \mathbb{N}$.

Аналогно $k\langle x,y\rangle$ садржи и потпрстен генерисан скупом $\{z_i|i \geqslant 0\}$ који је изоморфан са $k\langle x_0, x_1, \ldots\rangle$. Значи слободан k-прстен $k\langle x,y\rangle$ је коначно генерисан, а садржи потпрстен који је генерисан са пребројиво много неодређених. Претходно не важи ни у једном прстену полинома у ком неодређене комутирају. ▽

Пример 4. Нека је k прстен и $(G,\cdot)$ група. Елементи *групног прстена* kG су формалне суме $\sum_{\sigma\in G} a_\sigma\sigma$, $a_\sigma \in K$, које множимо користећи множење у G:

$$(\textstyle\sum_{\sigma\in G} a_\sigma\sigma)(\sum_{\tau\in G} b_\tau\tau) = \sum_{\mu\in G} c_\mu\mu, \quad \text{где је } c_\mu = \sum_{\substack{(\sigma,\tau)\in G^2 \\ \sigma\tau=\mu}} a_\sigma b_\tau.$$

Прстен kG је комутативан акко су и k и G комутативни. Претходно својство прстена kG чини га погодним за бројне конструкције некомутативних прстена. ▽

Пример 5. За произвољан прстен k дефинишемо прстен $k((x))$ *Лоранових редова* као скуп формалних редова $F = \sum_{-\infty}^{+\infty} f_i x^i$, у којима је само коначно много коефицијената $f_i \in k, i < 0$ различито од нуле. Редове множимо формално имајући у виду да елементи из k комутирају са x. ▽

Прстен R је *леви (десни) Нетерин* ако је сваки растући низ левих (десних) идеала у R стационаран или еквивалентно сваки леви (десни) идеал је коначно генерисан. Прстен R је Нетерин ако је и леви и десни Нетерин. Аналогно дефинишемо *Артинове* прстене захтевајући да је сваки опадајући низ одговарајућих идеала стационаран. Наредни пример показаће да су својства леве и десне "нетериности" независна.

Пример 6. Нека је σ ендоморфизам тела k који није аутоморфизам. Са $k[x,\sigma]$ означаваћемо прстен "десних" полинома по неодређеној x, $\sum x^i a_i$ које сабирамо на уобичајен начин, а множимо користећи закон дистрибутивности и правило $ax = x\sigma(a), a \in k$. Прстен $R = k[x,\sigma]$ је десни Нетерин, али не и леви. Ако је I десни идеал у R и f моничан полином најмањег степена у I, применом Еуклидовог алгоритма следи $I = fR$, то јест R је десни главноидеалски, тиме и десни Нетерин. С друге стране за фиксиран елемент $b \in k \setminus \sigma(k)$, директна сума левих идеала $\sum_{i=0}^{+\infty} Rxbx^i$ је леви идеал у R, који није коначно генерисан. То ће потврдити да R није леви Нетерин. Претпоставимо супротно да у R постоји једнакост

$$f_n(x)xbx^n + \cdots + f_{n+m}(x)xbx^{n+m} = 0$$

у којој су први и последњи сабирак различити од нуле. Како је R домен то је $f_n(x)xb = g(x)x$ за неко $g(x) = \sum x^i a_i \in R$. Ако је $f_n(x) = x^r c_r + \ldots, c_r \neq 0$ (тачкице означавају факторе нижег степена), изједначавањем коефицијената уз x^{r+1} добијамо $\sigma(c_r)b = \sigma(a_r)$, што је у контрадикцији са претпоставком $b \notin \sigma(k)$. ▽

Рангом врста матрице A формата $m \times n$ над телом K зваћемо димензију левог K-*простора врста* матрице A то јест потпростора левог

простора K^n разапетог над врстама матрице A. *Ранг колона* и *простор колона* дефинишемо слично, само уместо левих простора сада посматрамо десне. На основу познатог става из линеарне алгебре, ранг врста и ранг колона произвољне матрице над комутативним телом су једнаки. Претходно важи и у некомутативном случају и доказ који ћемо овде приказати јасно показује да претпоставка комутативности у овом тврђењу није неопходна. Нека је r ранг врста матрице A, c ранг колона и $B \in M_{rn}(K)$ матрица чијих r врста чини базу (левог) простора врста матрице A. Изражавајући врсте матрице A као леве линеарне комбинације врста матрице B, добијамо $A = B'B$ за одговарајућу матрицу $B' \in M_{mr}(K)$. Ова једнакост такође показује да су колоне матрице A десне линеарне комбинације r колона матрице B', одакле је $c \leqslant r$. Аналогно је и $r \leqslant c$, па важи једнакост. Заједничку вредност ранга врста и колона матрице A зваћемо *рангом* матрице A. При том је квадратна матрица формата $n \times n$ инвертибилна у прстену $M_n(K)$ акко је ранга n. Нагласимо да ранг матрице A у општем случају не мора бити једнак димензији потпростора десног простора K^n разапетог над врстама матрице A. Другим речима, ранг матрице A не мора бити једнак рангу матрице A^T. Ову чињеницу поткрепиће следећи пример:

Пример 7. За $a, b \in K$, матрица $A = \begin{bmatrix} 1 & b \\ a & ab \end{bmatrix}$ је ранга 1, док је $A^T = \begin{bmatrix} 1 & a \\ b & ab \end{bmatrix}$ ранга 2, уколико је $ab \neq ba$. Отуда једнакост

$$\operatorname{rang} A = \operatorname{rang} A^T$$

важи акко је K поље. ∇

1.2 Ореови домени

У комутативној алгебри сваки комутативан домен можемо утопити у његово поље разломака, које је при том јединствено одређено до на изоморфизам. Поставља се питање да ли аналогно важи и у некомутативној алгебри, то јест да ли за произвољан некомутативан домен постоји тело разломака и уколико постоји да ли је јединствено одређено. Одговор на оба питања је: не. Постоје некомутативни домени који се не могу утопити у тело, а такође постоје и домени који имају више неизоморфних тела разломака. Међутим за једну класу некомутативних домена важе ставови аналогни онима у комутативном случају.

Домен R је *леви Ореов* ако за свака два елемента $a, b \in R$, $a, b \neq 0$ важи $Ra \cap Rb \neq \{0\}$. Аналогно дефинишемо *десне Ореове* домене. Домен је *Ореов* ако је и леви и десни Ореов. Значај Ореових домена је у Ореовој конструкцији тела разломака за дати на пример десни Ореов домен. Ова конструкција је веома слична конструкцији поља разломака произвољног комутативног домена. Она се састоји у следећем: у скупу свих уређених парова $(a, b) \in R \times (R \setminus \{0\})$ дефинишемо релацију $\sim$ са $(a, b) \sim (c, d)$ акко постоје $s, t \in R \setminus \{0\}$ за које је $as = ct$ и $bs = dt$. Уведена релација $\sim$ је релација еквиваленције на скупу $R \times (R \setminus \{0\})$. Одговарајући количнички скуп означаваћемо са K, а класу $(a, b)/\sim$ са a/b. Приметимо

да је допуштено проширивање и скраћивање разломака, али само са десне стране: $ac/bc = a/b$ за $c \in R \setminus \{0\}$. Како је R десни Ореов свака два не нула елемента из R имају заједнички десни садржалац, који је различит од нуле. То ће нам омогућити да на K уведемо сабирање и множење. Наиме, за $a/b, c/d \in K$, постоје $s, t \in R \setminus \{0\}$ за које је $bs = dt = u$, па сабирање дефинишемо са $a/b + c/d = (as + ct)/u$. Слично, за $a/b, c/d \in K$, дефинишемо $a/b \cdot c/d = 0$ за $c = 0$, а ако је $c \neq 0$, постоје $s, t \in R \setminus \{0\}$ за које је $bs = ct = u$ и у том случају дефинишемо $a/b \cdot c/d = as/dt$. У односу на овако дефинисане операције сабирања и множења скуп K је тело, а пресликавање $a \mapsto a/1$ задаје утапање десног Ореовог домена R у тело K и притом је $a/b = a \cdot b^{-1}$ за $a, b \in R$. Дакле, сваки десни Ореов домен можемо утопити у тело. Отуда сваки десни Ореов домен поседује бар једно тело разломака, које је при том и јединствено одређено до на изоморфизам (доказ [8]).

Мултипликативни подскуп S домена R зовемо *десним Ореовим* скупом ако је $sR \cap aS \neq \{0\}$ за свако $a \in R$ и свако $s \in S$. Значај Ореових скупова је у конструкцији *локализације* R_S прстена R по датом Ореовом скупу S. Ова конструкција описана је у следећој теореми:

Теорема 1. *Нека је S десни Ореов скуп домена R. Релација $\sim$ скупа $R \times S$ дефинисана са:*

$$(a, s) \sim (a', s') \quad \textit{кад год је} \quad au = a'u', su = s'u' \quad \textit{за неке} \quad u, u' \in R$$

је релација еквиваленције. □

Количнички скуп $R \times S$ означаваћемо са R_S, а његове елементе као разломке $a/s = as^{-1}$. Скуп R_S је прстен у односу на операције сабирања и множења дефинсане аналогно као при конструкцији тела разломака датог Ореовог домена.

1.3 Факторизација, главноидеалски прстени

Ово поглавље посветићемо факторизацији у некомутативним прстенима и то посебно у главноидеалским. На почетку уводимо неколико појмова које ћемо користити у новим уопштеним дефиницијама одговарајућих комутативних појмова.

Асоцирани елементи

За елементе a, a' прстена R кажемо да су *асоцирани* ако постоје инвертибилни $p, q \in R$ за које је $a' = paq$. У прстенима матрица уводимо и појам *слабе асоцираности*. Матрице A и A' су *слабо асоциране* ако су матрице $A \oplus E$ и $A' \oplus E$ асоциране (са E смо означили јединичне матрице које не морају обавезно бити истих формата).

Пример 1. Матрица

$$A = P^{-1} \cdot \begin{bmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & k \end{bmatrix} \cdot Q \in M_n(R)$$

је слабо асоцирана са $k \in R$.

∇

Копроста релација

За релацију

$$ab' = ba'$$

у прстену R кажемо да је *копроста*, уколико су a, b *лево копрости* (немају заједничких неинвертибилних левих фактора), а a', b' су *десно копрости*. Свака два десно *комаксимална* елемента a, b $(aR + bR = R)$ су лево копроста. У главноидеалским доменима важи и обрат. Наиме, ако су a, b лево копрости из $aR + bR = dR$ следи да је d јединица и отуда $aR + bR = R$.

Пример 2. Релација

$$(1 + xy)x = x(1 + yx) \tag{1}$$

је копроста у прстену $k\langle x, y\rangle$. Елементи $1 + xy$ и x су лево копрости, јер су десно комаксимални $(1 + xy)R + xR = R$. Аналогно су x и $1 + yx$ лево комаксимални и десно копрости.

∇

Нека је R надаље домен. За елементе $a, a' \in R^\times$ посматраћемо хомоморфизам модула

$$f : R/Ra \longrightarrow R/Ra'. \tag{2}$$

Ако $1 \mapsto b'$, онда $x \mapsto xb'$ и како $a \mapsto 0$ то $ab' \in Ra'$, рецимо:

$$ab' = ba'. \tag{3}$$

Отуда је хомоморфизам f задат релацијом (3), и обратно, свака релација (3) задаје хомоморфизам f. При том је елемент b' одређен до на елемент из Ra'. За $b'_1 = b' + za'$ је

$$ab'_1 = a(b' + za') = ba' + aza' = (b + az)a',$$

па је b одређен до на елемент из Ra. Из претходног је релацијом (3) такође одређен и јединствен R-хомоморфизам

$$f^* : R/a'R \longrightarrow R/aR, \quad x \mapsto bx. \tag{4}$$

Модуле облика R/Ra или R/aR, $a \neq 0$ зваћемо *стриктно цикличним*. Из претходног следи да су категорије левих и десних цикличних модула над доменима дуалне.

Пресликавање (2) је инјективно, ако $xb' \in Ra'$ повлачи $x \in Ra$, то јест ако је релацијом (3) задат најмањи заједнички леви садржалац елемената a' и b'. У том случају релација (3) је лево копроста. За сурјективност f неопходна је егзистенција елемента $c \in R$ за који је $f(c) = 1$ то

јест $cb' - 1 \in Ra'$. У том случају релација (3) је лево комаксимална, јер постоји $d \in R$ за који је

$$da' + cb' = 1.$$

Ако је R главноидеалски домен пресликавање (2) је изоморфизам акко је релација (3) комаксимална.

Тврђење 1. *За елементе $a, a' \in R^\times$ главноидеалског домена R следећи услови су еквивалентни:*

а) постоји копроста релација (3);
б) постоји комаксимална релација (3);
в) $R/Ra \cong R/Ra'$;
г) $R/aR \cong R/a'R$.

□

Слични елементи

За елементе a, a' прстена R рећи ћемо да су *слични* ако задовољавају услов б) претходног тврђења. У комутативном случају сличност се своди на асоцираност (a, a' разликују се до на инвертибилан елемент).

Пример 3. Релација (1) у примеру 1. је комаксимална, па су елементи $1 + xy$ и $1 + yx$ слични у прстену $k\langle x, y\rangle$. ▽

Пример 4. За $k = \mathbb{C}$ и $\sigma : \mathbb{C} \to \mathbb{C}$, $\sigma(a) = \overline{a}$, користећи конструкцију из примера 1.1.6. добијамо прстен $\mathbb{C}[x, -]$ *комплексно-косих* полинома. Његови елементи су облика

$$a_0 + xa_1 + \cdots + x^n a_n, \quad a_i \in \mathbb{C}$$

и важи једнакост $ax = x\overline{a}$. Релација

$$(x-1)(1+\sqrt{2}+i) = (1+\sqrt{2}-i)(x-(\frac{1}{\sqrt{2}}+\frac{i}{\sqrt{2}}))$$

је комаксимална у прстену $\mathbb{C}[x, -]$, па су елементи $x - 1$ и $x - (\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}})$ слични. Аналогно је $x - 1$ сличан сваком полиному облика $x - u$, за $\mid u \mid = 1$. ▽

Домени са једнозначном факторизацијом

Елемент прстена R је *атом* ако није инвертибилан и ако се не може представити као производ два неинвертибилна елемента. Ако је R главноидеалски домен и $a \in R^\times$ онда свакој факторизацији $a = p_1 \dots p_r$ на неинвертибилне факторе одговара ланац десних идеала

$$R \supset p_1 R \supset p_1 p_2 R \supset \cdots \supset p_1 \dots p_r R = aR, \tag{5}$$

где су све инклузије строге с обзиром на то да $p_i \notin R^\times$. Ако су сви p_i атоми онда је (5) композициони низ. На основу *Жордан-Хелдерове* теореме ([5]) примењене на два композициона низа $a = p_1 \dots p_r = p'_1 \dots p'_s$ је $r = s$ и за неку пермутацију $i \mapsto i'$ скупа $\{1, \dots, r\}$, p_i и $p'_{i'}$ су слични.

У овом случају за R кажемо да је домен са *једнозначном факторизацијом*, а за факторизације $a = p_1 \dots p_r$ и $p'_1 \dots p'_r$ да су *изоморфне*. Овом дефиницијом обухваћен је и комутативан случај. Наиме, у комутативним доменима ова дефиниција еквивалентна је класичној дефиницији домена са јединственом факторизацијом. Дужину композиционог низа (5) зваћемо *дужином* елемента a.

Пример 5. *Прстен полинома над телом кватерниона* $R = \mathbb{H}[t]$
Реч је о обичним полиномима, у којима неодређена t комутира са коефицијентима из тела $\mathbb{H}$. Као прстен полинома над телом, R је главноидеалски, тиме и са јединственом факторизацијом. У овом прстену полином $t^2 + 1$ има бар три нетривијалне факторизације:

$$(t-i)(t+i), \quad (t-j)(t+j), \quad (t-k)(t+k).$$

Међутим, све три су изоморфне. Из комаксималне релације

$$(t-i)(t+i) = (t+j)(t-j)$$

следи сличност полинома $t-i$ и $t-j$. Аналогно за остале случајеве. ∇

Пример 6. Из примера 4. следи да полином $x^2 - 1$ у прстену $\mathbb{C}[x, -]$ има бесконачно много нетривијалних изоморфних факторизација облика $(x-u)(x+\overline{u})$ за $|\, u \,| = 1$.
∇

Пример 7. *Вејлова алгебра над телом* K
је количнички прстен $A_1(K) = K\langle x, y\rangle / \langle xy - yx - 1\rangle$. Релација

$$(1+xy)x = x(1+yx) = x(xy)$$

је комаксимална у $A_1(K)$, па су елементи $1+xy$ и xy слични. Приметимо да је $1+xy$ атом, док xy није. То ће посебно значити да $A_1(K)$ није прстен са јединственом факторизацијом. Примера ради елемент $xyx + x$ има две факторизације $(1+xy)x$ и x^2y у $A_1(K)$ различитих дужина. ∇

Сопствени прстен идеала

Нека је R домен. За $a = a'$ пресликавање (2) је ендоморфизам левог модула R/Ra и задато је елементом b' за који је $ab' = ba$, за неко $b \in R$. *Идеализатором* левог идеала Ra зваћемо највећи потпрстен прстена R који садржи Ra као свој идеал:

$$\mathcal{J}(Ra) = \{b' \in R |\ \ ab' \in Ra\}.$$

Применом претходног, постоји епиморфизам $\mathcal{J}(Ra)$ на $\mathrm{End}_R(R/Ra)$ који $b' \in \mathcal{J}(Ra)$ слика у ендоморфизам $x \mapsto xb'$. Језгро овог пресликавања је Ra и отуда је

$$\mathrm{End}_R(R/Ra) \cong \mathcal{J}(Ra)/Ra.$$

Количнички прстен $\mathcal{J}(Ra)/Ra$ зваћемо *сопственим* прстеном идеала Ra.

Пример 8. У прстену $R = \mathbb{C}[x, -]$ идеализатор идеала $R(x^2+1)$ је цео прстен R. Како је x^2+1 атом у R то је сопствени прстен овог идеала тело. Слично је $\mathcal{J}(R(x^2-1)) = R$. Како x^2-1 није атом то сопствени прстен у овом случају није тело. Међутим, важи следеће:

$$\mathcal{J}(R(x^2-1))/R(x^2-1) = R/R(x^2-1) \cong M_4(\mathbb{C}).$$

∇

Инваријантни елементи

За елемент c прстена R кажемо да је *десно инваријантан* ако је десно регуларан и $Rc \subseteq cR$, што значи да за свако $x \in R$ постоји јединствен $x' \in R$ за који је $xc = cx'$. Леву инваријатност дефинишемо слично. Елементе који су и лево и десно инваријантни зовемо *инваријантним*. Приметимо да инваријантни елементи генеришу двостране идеале.

Пример 9. Полином x^2+1 је инваријантан у прстену $R = \mathbb{C}[x, -]$, јер за свако $p \in R$ важи $(x^2+1) \cdot p = p \cdot (x^2+1)$. Уопште, сваки полином облика $p(x^2)$ инваријантан је у R. ∇

Пример 10. У прстену *интегралних кватерниона*

$$\mathbb{I} = \mathbb{Z}1 \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k$$

важи:

$$i(1+ai+bj+ck) = (1+ai+bj+ck)(qi+rj+sk)$$

за

$$q = 1-(b^2+c^2)u, \quad r = (ab-c)u, \quad s = (ac+b)u, \quad u = 2(1+a^2+b^2+c^2)^{-1}.$$

Аналогне релације важе и за множење слева елементима j и k. Отуда је елемент $1+ai+bj+ck$ инваријантан у $\mathbb{I}$ акко је облика $\mu(1+i+j+k)$ за $\mu \in \mathbb{Z}$ или ν за $\nu \in \mathbb{Z}$. ∇

За елемент a прстена R рећи ћемо да је *ограничен* уколико је леви фактор неког инваријантног елемента: $c = ab$, где је c инваријантан; a је такође и десни фактор c: $cb = b'c = b'ab$ и отуда $c = b'a$, што показује да је појам ограничености симетричан. Сваки инваријантан елемент коме је a леви фактор зваћемо *границом* елемента a. У општем случају најмања граница не мора да постоји. У главноидеалским доменима постоји и то је инваријантни генератор a^* максималног идеала садржаног у Ra и јединствено је одређена до на инвертибилан елемент. Може се још окарактерисати и као генератор идеала $\mathrm{Ann}(R/Ra)$. То значи да је сваки елемент сличан a ограничен и то истим границама. Елементе без ограничених фактора зовемо *тотално неограниченим*.

Пример 11. У прстену $\mathbb{C}[x, -]$ елемент $x-i$ је ограничен, јер је фактор инваријантног полинома x^2-1. ∇

Инваријантан елемент $c \in R$ зовемо *I-атомом* ако $c \notin R^\times$ и ако су његови једини инваријантни фактори њему асоцирани или јединице.

Пример 12. Полином x^2+1 је I-атом у прстену $\mathbb{C}[x,-]$. ▽

Веза између уведених појмова над главноидеалским доменима наведена је у наредној теореми (доказ [8]).

Теорема 2. *Нека је R главноидеалски домен.*

а) Сваки идеал $I \neq 0$ у R је облика $cR = Rc$ за неки инваријантан елемент $c \in R$; прстен R/Rc је прост акко је c I-атом;
б) сваки I-атом је производ сличних ограничених атома;
в) ако је p ограничен атом онда је његова најмања граница p^* I-атом коме су сви атомични фактори слични p. □

1.4 Редукција матрица над главноидеалским доменима

У прстену R у ком је сваки идеал слободан као леви или десни модул за сваку матрицу $A \in M_{mn}(R)$ постоје инвертибилне матрице $P \in GL_m(R)$ и $Q \in GL_n(R)$ за које је $PAQ = A_1 \oplus 0$ за неку регуларну матрицу A_1. У општем случају даље редукције нису могуће. Али, ако је R главноидеалски домен A је могуће редуковати до дијагоналне матрице. У вези са тим увешћемо следећу дефиницију. За елемент a произвољног домена R кажемо да је *тотални* дивизор елемента $b \in R$ и пишемо $a \parallel b$, ако постоји елемент $c \in R$ за који $a \mid c \mid b$ (мисли се на дељивост слева). Приметимо да у општем случају произвољан елемент није тотални дивизор самог себе. Заправо $a \parallel a$ акко је a инваријантан. У простом прстену R немамо неинвертибилних инваријантних елемената, јер релација $a \parallel b$ важи једино за $a \in R^\times$ или $b = 0$.

Са $\operatorname{diag}(a_1, \ldots, a_r)$ означаваћемо дијагоналну матрицу са елементима $a_1, \ldots, a_r$ на главној дијагонали. Ову ознаку користићемо и за матрице које нису квадратне, што ће бити посебно наглашено истицањем њиховог формата.

Теорема 1. *Нека је R главноидеалски домен. Ранг врста и колона произвољне матрице $A \in M_{mn}(R)$ су једнаки; ако је њихова заједничка вредност рецимо r, онда постоје $P \in GL_m(R), Q \in GL_n(R)$ за које је*

$$P^{-1}AQ = \operatorname{diag}(e_1, \ldots, e_r, 0, \ldots, 0), \quad e_i \parallel e_{i+1}, \quad e_r \neq 0.$$

Доказ: Користићемо следеће операције на колонама матрице A:

1) замена две колоне,
2) множење здесна инвертибилним елементом,
3) додавање i-тој колони j-те помножене здесна неким елементом из R,
4) множење две колоне здесна инвертибилном 2×2 матрицом.

Свакој од операција 1) – 3) одговара множење здесна елементарним матрицама. Операција 4) омогућава замену прва два елемента у одабраним колонама, редом, њиховим највећим заједничким левим фактором и нулом. Ако су то нпр. елементи a, b онда из $aR + bR = kR$ следи

$a = ka_1, b = kb_1$, што значи да су a_1, b_1 десно копрости тј. да постоје $d', c' \in R$ за које је

$$a_1 d' - b_1 c' = 1. \tag{1}$$

Скуп $\{x \in R \mid b_1 x \in a_1 R\}$ је идеал у R и нека је нпр. генерисан елементом a'. Како $a' \in a'R$, то је

$$b_1 a' = a_1 b' \tag{2}$$

за неко $b' \in R$. Множењем здесна релације (1) са a_1 добијамо

$$a_1(d' a_1 - 1) = b_1 c' a_1,$$

и тиме $c' a_1 \in a' R$ тј.

$$c' a_1 = a' c \tag{3}$$

за неко $c \in R$. Аналогно множењем сада релације (1) здесна са b_1 закључујемо да $1 + c' b_1 \in a_1 R$ и отуда $a' d - c' b_1 = 1$ за неко $d \in R$. За матрице μ, ν задате са:

$$\mu = \begin{bmatrix} a_1 & b_1 \\ c & d \end{bmatrix}, \qquad \nu = \begin{bmatrix} d' & -b' \\ -c' & a' \end{bmatrix}$$

је

$$\mu\nu = \begin{bmatrix} 1 & 0 \\ * & * \end{bmatrix}, \qquad \nu\mu = \begin{bmatrix} * & * \\ 0 & 1 \end{bmatrix}.$$

За $f_1 = [1, 0], f_2 = [0, 1]$ важи $f_1(\mu\nu - E) = 0$ и $f_2(\nu\mu - E) = 0$, као и

$$f_2\nu(\mu\nu - E) = f_2(\nu\mu\nu - \nu) = f_2(\nu\mu - E)\nu = 0.$$

Заменом матрица μ и ν у претходној једнакости добијамо

$$[-c', a'] \begin{bmatrix} 0 & 0 \\ u & v \end{bmatrix} = [a'u, a'v] = 0$$

за неке $u, v \in R$ и отуда $u = v = 0$, што за последицу има $\mu\nu = E$. Аналогно је $\nu\mu = E$. Сада важи $[k, 0]\mu = [a, b]$ и $[a, b]\nu = [k, 0]$ што смо и захтевали. Одговарајуће операције можемо примењивати и на врсте, с тим што је свако множење слева.

Сада можемо наставити са редукцијом. Ако је $A = 0$, крај. Иначе, користећи 1), пермутовањем врста и колона на $(1, 1)$ позицију постављамо елемент који је различит од нуле. Даље, користећи 4), a_{11} мењамо највећим заједничким левим фактором a_{11} и a_{12}, затим a_{11} и a_{13} итд.. Након $n - 1$ корака A редукујемо до матрице у којој је $a_{12} = \cdots = a_{1n} = 0$. Исти поступак применимо и на прву колону. Међутим, може се догодити да током ове редукције прва врста опет постане различита од нуле. Да би ово избегли, доказ изводимо индукцијом по дужини a_{11} и тако добијамо

$$A = a_{11} \oplus A_1.$$

Другом индукцијом, по $\max(m, n)$ добијамо

$$A = \operatorname{diag}(a_1, a_2, \ldots, a_t, 0, \ldots, 0).$$

За свако $d \in R$ је

$$\begin{bmatrix} 1 & d \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a_1 & 0 \\ 0 & a_2 \end{bmatrix} = \begin{bmatrix} a_1 & da_2 \\ 0 & a_2 \end{bmatrix},$$

тако да се опет може нарушити дужина a_1 осим ако је a_1 леви фактор da_2 за све $d \in R$, тј. $a_1R \supseteq Ra_2$. У том случају је $a_1R \supseteq Ra_2R \supseteq Ra_2$; и $a_1 \mid c \mid a_2$, где је c инваријантан генератор идеала Ra_2R. Отуда $a_1 \parallel a_2$. Понављањем претходног добијамо

$$\operatorname{diag}(e_1, e_2, \ldots, e_t, 0, \ldots, 0), \qquad \text{где} \quad e_i \parallel e_{i+1}.$$

Ако је $e_t \neq 0$ ранг врста и колона ове матрице је t. Како матрице A и $P^{-1}AQ$ имају једнаке рангове колона и врста, тврђење је доказано. □

Пример 1. У прстену $M_n(\mathbb{H}[t])$ матрица

$$A = \begin{bmatrix} tj-k & (t^2+1)(tj-i) & 0 \\ ti+1 & (t^2+1)(1-i) & (t^2+1)^2(-ti-k) \\ 0 & 0 & (t^2+1)^2 \end{bmatrix}$$

елементарним трансформацијама своди се на матрицу

$$\operatorname{diag}(t-i, (t^2+1)(t-j), (t^2+1)^2(t-k)).$$

При том

$$(t-i) \mid (t^2+1) \mid (t^2+1)(t-j),$$

па

$$(t-i) \parallel (t^2+1)(t-j),$$

јер је t^2+1 инваријантан у прстену $\mathbb{H}[t]$. Аналогно $(t^2+1)(t-j) \mid (t^2+1)^2 \mid (t^2+1)^2(t-k)$, па $(t^2+1)(t-j) \parallel (t^2+1)^2(t-k)$, имајући у виду да је $(t^2+1)^2$ инваријантан у $\mathbb{H}[t]$. ▽

У наредном поглављу показаћемо да су e-ови јединствено одређени до на сличност. Уколико би R био Еуклидски домен, уместо 4) могао би се користити Еуклидов алгоритам, а уместо индукције по дужини могла би се користити индукција по степену.

Последица 2. *Свака матрица над простим главноидеалским доменом R асоцирана је матрици $E \oplus a \oplus 0$ за неко $a \in R$.*

Доказ: Као што смо видели у простом прстену R релација $a \parallel b$ повлачи $b = 0$ или $a \in R^\times$. Користећи 2) сваки инвертибилан елемент можемо трансформисати у 1, тако да на дијагонали трансформисане матрице само један елемент може бити различит од нуле. □

У телима, сваки не нула елемент је инвертибилан, па је у овом случају свака матрица асоцирана некој матрици облика $E_r \oplus 0$, где је r ранг матрице A.

За R-модул M кажемо да је *коначно презентован* ако постоји тачан низ облика:

$$R^m \xrightarrow{\alpha} R^n \longrightarrow M \longrightarrow 0.$$

На овај начин M је одређен једнозначно до на изоморфизам матрицом A формата $m \times n$ којом је задато пресликавање α. Обратно, свака $m \times n$ матрица дефинише коначно презентован модул M одређен са $M = \operatorname{coker} \alpha$. Асоцираним матрицама одговарају изоморфни модули, јер се на овај начин заправо задаје промена база модула R^m и R^n.

Нека је сада $R = K[t]$, где је K тело и $f \in R$ полином степена d. R-модул $M = R/fR$ је и K-простор димензије d. Општије, нека је M десни R-модул дефинисан матрицом A. Ако је A регуларна M је коначнодимензиони K-простор и његова димензија је управо $\deg f_1 \dots f_r$, где је $f_1 \dots f_r$ производ дијагоналних компоненти матрице добијене редукцијом A.

1.5 Коначно генерисани модули над главноидеалским доменима

Сваки коначно генерисан модул над комутативним главноидеалским прстеном је директна сума цикличних. Природно се намеће питање, да ли аналогно важи и у некомутативном случају. Одговор је потврдан.

За модул M кажемо да је *торзиони* ако се сваки његов елемент анулира неким не нула елементом из R. Ако претходно не важи ни за један елемент модула M осим за нулу, за M кажемо да је *торзионо слободан*. Аналогно, као код Абелових група, сваки модул M над главноидеалским прстеном садржи јединствено одређен максимални торзиони подмодул tM (R је и леви Ореов прстен, па је tM подмодул модула M). При том је M/tM торзионо слободан. Ако је M коначно генерисан, онда је то и слободан модул M/tM. Отуда је $M = tM \oplus F$, где је F слободан подмодул, јединствено одређен до на изоморфизам (доказ [6]).

Теорема 1. *Сваки коначно генерисан модул M над главноидеалским прстеном R је директна сума цикличних модула:*

$$M \cong R/Re_1 \oplus \cdots \oplus R/Re_r \oplus R^{m-r}, \tag{1}$$

где $e_i \mid\mid e_{i+1}$. Овим условом е-ови су јединствено одређени до на сличност.

Доказ: Модул M је коначно генерисан, тиме и коначно презентован, рецимо матрицом A. По теореми 1.4.1. матрица A је асоцирана матрици $\operatorname{diag}(e_1, \dots, e_r, 0, \dots, 0)$, при чему $e_i \mid\mid e_{i+1}$. Како ове промене не утичу на модул M, преостаје једино да покажемо јединственост.

Користићемо следеће тврђење: Ако су M, N, N' коначно генерисани модули над R, за које је $M \oplus N \cong M \oplus N'$, онда је $N \cong N'$ (доказ [6]). Директну суму $R/Ra_1 \oplus \cdots \oplus R/Ra_k$ записаћемо краће $[a_1, \dots, a_k]$, док ћемо са $\sim$ означавати изоморфност. Тако је $[a] \sim [b]$ акко су a и b слични. Још треба показати да важи следећа импликација:

$$[a, b_1, \dots, b_r] \sim [a, b'_1, \dots, b'_s] \Rightarrow [b_1, \dots, b_r] \sim [b'_1, \dots, b'_s].$$

Нека су $[d_1, \dots, d_r]$, $d_i \mid\mid d_{i+1}$ и $[e_1, \dots, e_r]$, $e_i \mid\mid e_{i+1}$ две репрезентације модула M. Без умањења општости можемо претпоставити да је број сабирака на левој и десној страни једнак, с обзиром на то да увек можемо додати нуле, које су репрезентоване инвертибилним факторима ($R/R = 0$).

Даље, можемо претпоставити да је торзиони део модула M одбачен, тако да су сви $d_i, e_i \neq 0$. Како за $r = 1$ тврђење важи, претпоставимо да је $r > 1$. Доказ ћемо извести индукцијом по r. Означимо са $l(a)$ дужину елемента a и претпоставимо да је $l(d_1) \geqslant l(e_1)$; даље $d_1 \mid c \mid d_2$ и c је инваријантан. За $N = R/Ra$ и c инваријантан важи $N/cN \cong R/(Ra + Rc)$. Ако је $Re_i \oplus Rc = Re_i'$, онда је:

$$M/cM \sim [d_1, c, \ldots, c] \sim [e_1', \ldots, e_r'], \tag{2}$$

и $l(e_i') \leqslant l(c)$ $(i = 1, \ldots, r)$, $l(e_1') \leqslant l(e_1) \leqslant l(d_1)$. Упоређивањем дужина у (2) које морају бити једнаке, као дужине композиционих низова модула M/cM, добијамо $l(d_1) + (r-1)l(c) = \sum l(e_i')$, то јест

$$(l(d_1) - l(e_1')) + \sum_{2}^{r} (l(c) - l(e_i')) = 0.$$

Како је сваки терм ненегативан, сви фактори су нуле. Отуда је $l(e_1') = l(e_1) = l(d_1)$, $l(e_i') = l(c)$, одакле следи $e_1' \sim e_1, e_i' \sim c$ $(i > 1)$. Сада је (2) облика:

$$[d_1, c, \ldots, c] \sim [e_1, c \ldots, c].$$

Скраћивањем, налазимо да је e_1 сличан са d; тако да сада можемо скратити први терм у $[d_1, \ldots, d_r] \sim [e_1, \ldots, e_r]$ на обе стране. Тиме смо добили $[d_2, \ldots, d_r] \sim [e_2, \ldots, e_r]$. Индукција по r даје тражени резултат. □

Следећа теорема даје опис структуре коначно генерисаних цикличних модула над главноидеалским доменима (доказ [6]).

Теорема 2. *Нека је R главноидеалски домен. Сваки цикличан леви R-модул је или слободан ранга 1 или облика*

$$R/Ra \cong R/Rq_1 \oplus \cdots \oplus R/Rq_k \oplus R/Rq, \tag{5}$$

где је сваки q_i производ ограничених сличних атома и међу атомима у различитим q_i нема сличних, а q је тотално неограничен. Елементи $q_1, \ldots, q_k, q$ су јединствено одређени до на редослед и сличност. □

Претходне две теореме дају комплетан опис структуре коначно генерисаних модула над главноидеалским прстенима.

1.6 Основни појмови теорије тела

Адитивни и мултипликативни комутатори

У овом поглављу изложићемо основне резултате теорије тела. За елементе a, b тела K елемент $ab - ba$ зваћемо *адитивним комутатором*. Уколико су $x, y \in K^\times$ елемент $x^{-1}y^{-1}xy$ зваћемо *мултипликативним комутатором*.

Тврђење 1. *Ако елемент y тела K комутира са свим адитивним комутаторима у K, онда је y у центру C тела K.*

Доказ: Претпоставимо да $y \notin C$. Онда је $xy \neq yx$ за неко $x \in K$. Посматрамо једнакост:

$$x(xy) - (xy)x = x(xy - yx).$$

Пошто y комутира са адитивним комутаторима $x(xy) - (xy)x$ и $xy - yx \neq 0$, мора комутирати и са x. Контрадикција! □

Последица 2. *Ако су сви адитивни комутатори тела K централни, онда је K поље.* □

Последица 3. *Тело K је генерисано свим својим адитивним комутаторима и центром.*

Доказ: Ако $x \notin C$, онда је $xy \neq yx$ за неко $y \in K$. Сада C-алгебра генерисана адитивним комутаторима тела K садржи $x(xy) - (xy)x$ и $xy - yx \neq 0$, стога садржи и x, па је једнака K. □

Показаћемо да тврђења аналогна претходним важе и за мултипликативне комутаторе. Пре тога извешћемо неколико идентитета. Нека су a, c два елемента тела K који не комутирају и $b = a - 1 \in K^\times$. Тада је

$$\begin{aligned} a(a^{-1}ca - b^{-1}cb) &= ca - ab^{-1}cb \\ &= c(b+1) - (b+1)b^{-1}cb \\ &= c - b^{-1}cb \neq 0, \end{aligned} \tag{1}$$

и отуда

$$a(a^{-1}cac^{-1} - b^{-1}cbc^{-1}) = 1 - b^{-1}cbc^{-1} \neq 0. \tag{2}$$

У оба случаја десне стране једнакости су различите од нуле пошто $b = a - 1$ не комутира са c.

Тврђење 4. *Ако елемент c тела K комутира са свим мултипликативним комутаторима у K онда је c у центру тела K.*

Доказ: Претпоставимо супротно, да је $ac \neq ca$ за неко $a \in K$. Нека је $b = a - 1 \in K^\times$. Пошто по претпоставци c комутира и са $a^{-1}cac^{-1}$ и са $b^{-1}cbc^{-1}$, из једнакости (2) следи да c комутира и са a. Контрадикција! □

Последица 5. *Ако су сви мултипликативни комутатори тела K централни, онда је K поље.* □

За тело $D \subset K$ кажемо да је нормално у телу K ако је за свако $x \in K^\times$, $xDx^{-1} \subseteq D$, тј. ако је $D^\times$ нормална подгрупа групе $K^\times$.

Теорема 6. *Ако је тело $D \neq K$ нормално у телу K, онда је D садржано у центру тела K.*

Доказ: Нека је $a \in K \setminus D$ и $c \in D$. Тада је $ac = ca$. У супротном за $b = a - 1 \in K^\times$, $a^{-1}ca$, $b^{-1}cb$, c припадају $D^\times$. Сада из једнакости (1) следи да је и a у $D^\times$, што је у контрадикцији са полазном претпоставком. Нека је сада c' произвољан елемент из $D^\times$. Онда су и a и ac' у $K \setminus D$, па према претходном комутирају са c. У том случају и $c' = a^{-1}ac'$ комутира са c. Отуда c припада центру тела K, што је и требало показати. □

Последица 7. *Некомутативно тело K генерисано је свим својим мултипликативним комутаторима.*

Доказ: Нека је D подтело тела K генерисано свим мултипликативним комутаторима тела K. Тело D је инваријантно у односу на све унутрашње аутоморфизме тела K, па је нормално у K. Како K није комутативно то на основу последице 1.6.5 постоји мултипликативни комутатор који није централан. Отуда $D \not\subseteq C$. Сада је основу теореме 1.6.6. $K = D$ □

Изоморфизми и анти-изоморфизми

Пресликавање f тела K у неко тело D које је инјективно, сурјективно и сагласно са сабирањем зовемо *изоморфизмом* ако је

$$f(ab) = f(a)f(b), \quad \text{за свако} \quad a, b \in K.$$

Уколико је

$$f(ab) = f(b)f(a), \quad \text{за свако} \quad a, b \in K$$

пресликавање f зовемо *анти-изоморфизмом.*

Теорема 8. *Пресликавање σ тела K у тело D које има следеће особине:*

1) σ је сагласно са сабирањем,
2) за свако $a \neq 0$ је $\sigma(a^{-1}) = (\sigma(a))^{-1}$,
3) $\sigma(1) = 1$

је или изоморфизам или анти-изоморфизам тела K у тело D.

Примедба. Ако претпоставимо да σ испуњава само услове 1) и 2), онда за $x = \sigma(1)$ важи $x = x^{-1}$. Тада је $x^2 - 1 = (x-1)(x+1) = 0$. То јест, ако σ не испуњава услов 3), онда је $\sigma(1) = -1$. У овом случају пресликавање $\tau : K \to D$ задато са $\tau(a) = -\sigma(a)$ задовољава све услове теореме, што значи да је σ или опозит неког изоморфизма или неког анти-изоморфизма.

Доказ: Уместо $\sigma(a)$ писаћемо a^σ и аналогно $(a^{-1})^\sigma = (a^\sigma)^{-1}$ означићемо са $a^{-\sigma}$. Како је за $a \neq 0$, $a^\sigma \cdot a^{-\sigma} = 1$ то је $\ker\sigma = \{0\}$, па је σ 1 – 1 и на.

Прво ћемо извести један идентитет.

За $a, b \in K^\times$ и $a^{-1} \neq b$ израз $a^{-1} + (b^{-1} - a)^{-1}$ је добро дефинисан. Издвајањем a^{-1} слева и $(b^{-1} - a)^{-1}$ здесна добијамо

$$a^{-1} + (b^{-1} - a)^{-1} = a^{-1}((b^{-1} - a) + a)(b^{-1} - a)^{-1} = a^{-1}b^{-1}(b^{-1} - a)^{-1}. \quad (3)$$

И сада инвертовањем добијамо:

$$(a^{-1} + (b^{-1} - a)^{-1})^{-1} = (b^{-1} - a)ba = a - aba.$$

У вези са претходним је

$$a - (a^{-1} + (b^{-1} - a)^{-1})^{-1} = aba.$$

Ако сада применимо σ на претходну једнакост и при том искористимо услове 1) и 2) и једнакост (3) добићемо:

$$(aba)^\sigma = a^\sigma b^\sigma a^\sigma. \quad (4)$$

Једнакост (4) важи и за $a = b = 0$, као и у случају када је $a^{-1} = b$. Другим речима, под полазним претпоставкама, једнакост (4) је тачна за све $a, b \in K$.

За $b = 1$ из (4) следи

$$(a^2)^\sigma = (a^\sigma)^2. \tag{5}$$

Заменом a са $a + b$ у (5) добијамо:

$$(a^2 + ab + ba + b^2)^\sigma = (a^\sigma)^2 + a^\sigma b^\sigma + b^\sigma a^\sigma + (b^\sigma)^2.$$

Сада коришћењем (5) и услова 1) из претходне једнакости следи:

$$(ab)^\sigma + (ba)^\sigma = a^\sigma b^\sigma + b^\sigma a^\sigma. \tag{6}$$

За $a, b \in K^\times$ посматрамо елемент

$$((ab)^\sigma - a^\sigma b^\sigma)(ab)^{-\sigma}((ab)^\sigma - b^\sigma a^\sigma) \tag{7}$$

тела D. Множењем добијамо да је овај елемент једнак

$$(ab)^\sigma - b^\sigma a^\sigma - a^\sigma b^\sigma + a^\sigma b^\sigma (ab)^{-\sigma} b^\sigma a^\sigma. \tag{8}$$

Применом (4) је $b^\sigma (ab)^{-\sigma} b^\sigma = (b(ab)^{-1}b)^\sigma$, и

$$a^\sigma (b^\sigma (ab)^{-\sigma} b^\sigma) a^\sigma = (ba)^\sigma.$$

Тиме је (7) једнако са

$$(ab)^\sigma - b^\sigma a^\sigma - a^\sigma b^\sigma + (ba)^\sigma,$$

а то је 0 на основу једнакости (6). Отуда је бар један од фактора у (7) нула. То за последицу има да је

$$(ab)^\sigma = \begin{cases} a^\sigma b^\sigma \\ \text{или} \\ b^\sigma a^\sigma. \end{cases}$$

За $a = b = 0$ претходно тривијално важи. Сада се поставља питање: Да ли у K постоје четири елемента a, b, c, d за које је

$$\begin{array}{rcccl} (ab)^\sigma & = & a^\sigma b^\sigma & \neq & b^\sigma a^\sigma, \\ (cd)^\sigma & = & d^\sigma c^\sigma & \neq & c^\sigma d^\sigma \, ? \end{array} \tag{9}$$

Претпоставимо да такви елементи постоје. За $x \in K$ је

$$(a(b+x))^\sigma = \begin{cases} a^\sigma (b+x)^\sigma = a^\sigma b^\sigma + a^\sigma x^\sigma \\ \text{или} \\ (b+x)^\sigma a^\sigma = b^\sigma a^\sigma + x^\sigma a^\sigma. \end{cases}$$

У првом случају је $(ax)^\sigma = a^\sigma x^\sigma$, док из другог следи $(ax)^\sigma \neq x^\sigma a^\sigma$. То значи да за свако $x \in K$ важи $(ax)^\sigma = a^\sigma x^\sigma$. Аналогно долазимо до следећих једнакости:

$$(xb)^\sigma = x^\sigma b^\sigma,$$

$$(cx)^\sigma = c^\sigma x^\sigma,$$
$$(xd)^\sigma = x^\sigma d^\sigma.$$

Отуда је

$$a^\sigma d^\sigma = d^\sigma a^\sigma \quad \text{и} \quad c^\sigma b^\sigma = b^\sigma c^\sigma.$$

Из

$$((a+c)(b+d))^\sigma = \begin{cases} a^\sigma b^\sigma + a^\sigma d^\sigma + c^\sigma b^\sigma + c^\sigma d^\sigma \\ \text{или} \\ b^\sigma a^\sigma + d^\sigma a^\sigma + b^\sigma c^\sigma + d^\sigma c^\sigma. \end{cases}$$

директним рачунањем леве стране и изједначавањем са десном у првом случају добијамо $c^\sigma d^\sigma = d^\sigma c^\sigma$ што је у контрадикцији са (9). Аналогно у другом случају добијамо $a^\sigma b^\sigma = b^\sigma a^\sigma$, што је опет у контрадикцији са (9). Овим је доказ завршен. □

Касније ћемо на примеру показати примене претходне теореме у геометрији.

Уређена тела

За тело K кажемо да је *уређено* ако у K постоји непразан подскуп P који има следеће особине:

1) $K = -P \cup \{0\} \cup P$ (дисјунктна унија),
2) $P + P \subseteq P$,
3) $P \cdot P \subseteq P$.

Елементе скупа P зваћемо *позитивним* елементима. Уређење на телу K дефинишемо са

$$a > b \quad \text{акко} \quad a - b \in P.$$

Издвојићемо неколико особина овог уређења:

1) Ако је $c \in P$ и $a > b$ онда је $ac > bc$ и $ca > cb$. Аналогно за $-c \in P$ и $a > b$ је $bc > ac$ и $cb > ca$.

2) За свако $a \in K^\times$ је $a^2 > 0$. Посебно из $1^2 = 1$ следи да $1 \in P$. Отуда за $c > 0$ из $c^{-1} = c \cdot (c^{-1})^2$ следи да је и $c^{-1} > 0$. Аналогно из $c < 0$ следи $c^{-1} < 0$. Посебно, за $c \neq 0$ и $a > b$ је и $cac^{-1} > cbc^{-1}$. Из претходног за $b = 0$ и $b = 1$ добијамо $cPc^{-1} \subseteq P$ и $cSc^{-1} \subseteq S$, где је $S = \{a \in K \mid a > 1\}$.

Скуп P је једна подгрупа мултипликативне групе $K^\times$. При том је P дисјунктна унија $S \cup \{1\} \cup S^{-1}$, што значи да уређење на K индукује уређење мултипликативне групе P.

3) Како је $1 \in P$ то тело K мора бити карактеристике 0. Отуда су суме јединица увек позитивне. Стога уређење на K индукује стандардно уређење на подтелу Q које је изоморфно пољу рационалних бројева. То такође показује да се поље рационалних бројева може уредити само на уобичајен начин. Исто важи и за поље реалних бројева.

Архимедовска тела

За уређено тело кажемо да је *архимедовско* ако за свако $a \in K$ постоји цео број n за који је $a < n$. При том важи:

Теорема 9. *Свако архимедовско тело је комутативно и изоморфно неком подпољу поља реалних бројева, при чему је поље* $\mathbb{R}$ *уређено на стандардан начин.* □

Доказ ове теореме може се наћи у [3].

Наредни пример показаће да постоје и некомутативна уређена тела.

Пример 1. Нека је $\mathbb{Q}$ поље рационалних бројева и $K = \mathbb{Q}((x))$ скуп Лоранових редова са коефицијентима у $\mathbb{Q}$. Скуп K је тело у односу на сабирање и множење редова. Задаћемо уређење на K скупом P_0 позитивних елемената:

$$P_0 = \{\sum_{i=n}^{\infty} a_i x^i \mid n \in \mathbb{Z}, a_n > 0\}.$$

Нека је $\sigma : K \to K$ пресликавање задато са $\sigma(x) = 2x$. Приметимо да је σ аутоморфизам који чува уређење на K. Прецизније:

$$f = \sum_{i=n}^{\infty} a_i x^i \mapsto f^\sigma = \sum a_i 2^i x^i,$$

па пресликавање σ чува знак најнижег терма. Нека је сада $F = K((y))$ скуп десних Лоранових редова над телом K. Скуп F је некомутативно тело у односу на операције сабирања редова и множења које је задато правилом:

$$fy = yf^\sigma, \quad f \in K.$$

Ово тврђење биће доказано у поглављу 2.4.. Тело F означаваћемо са $K((y;\sigma))$ и зваћемо га телом *косих Лоранових* редова. Сада дефинишемо уређење на F скупом позитивних елемената

$$P = \{\sum_{i=n}^{\infty} y^i f_i \mid n \in \mathbb{Z}, f_n \in P_0\}.$$

Овај скуп је заиста скуп позитивних елемената тела F. Услови 1) и 2) очигледно важе. Показаћемо да је испуњен и услов 3), то јест да је производ два елемента скупа P опет у P. Нека су $f = \sum_{i=n}^{\infty} y^i f_i$, $g = \sum_{i=m}^{\infty} y^i g_i \in P$. То значи да су f_n и g_m из скупа P_0. Сада је коефицијент уз најнижи терм производа fg једнак $f_n^{\sigma^m} g_m$. Као што смо показали σ скуп P_0 слика у скуп P_0. То за последицу има да ће и производ $f_n^{\sigma^m} g_m$ бити елемент P_0, и тиме да је $fg \in P$. ▽

Тиме смо показали:

Теорема 10. *Постоје некомутативна уређена тела.* □

Примене у геометрији

За задато тело K посматрамо скуп

$$\mathcal{A} = K \times K = \{(\xi, \eta) \mid \xi, \eta \in K\}.$$

Елементе овог скупа зваћемо *тачкама*. Такође ћемо са (ξ, η) означавати и *векторе*. *Правом* ћемо звати подскуп l скупа $K \times K$ облика $P + tA$, где је

P задата тачка, A задати не нула вектор и $t \in K$. Пресликавања облика $\sigma(X) = \alpha X + C$ су *дилатације*. Оне имају следеће својство: За сваке две различите тачке P и Q и њихове слике P' и Q' свака права кроз P' паралелена са $P+Q$ пролази и кроз Q'. Свака дилатација различита од идентитете има највише једну фиксну тачку. Дилатације без фиксних тачака зовемо *транслацијама*. Оне су облика $\sigma(X) = X + C$. За овако уведене објекте важе све аксиоме афине геометрије, па је $(\mathcal{A}, \mathbb{V}, +)$ један *афини простор* ($\mathbb{V}$ означава скуп вектора).

За дилатацију σ кажемо да је *дегенеративна* ако је $\sigma(X) = P$ за свако $X \in \mathcal{A}$. За не-дегенеративну дилатацију σ *трагом* тачке P звaћемо праву која садржи тачке P и $\sigma(P)$.

Нека је сада T скуп свих транслација уоченог афиног простора. За пресликавање $\alpha : T \to T$ кажемо да је хомоморфизам који чува траг ако је:

1) α хомоморфизам, тј. $(\tau_1\tau_2)^\alpha = \tau_1^\alpha \tau_2^\alpha$

2) τ и τ^α имају исте трагове.

Скуп пресликавања са овим особинама означићемо са k. За пресликавања α и β скупа k конструишемо ново, које елемент τ скупа k слика у $\tau^\alpha \circ \tau^\beta$. Ово пресликавање означићемо са $\alpha + \beta$,

$$\tau^{\alpha+\beta} = \tau^\alpha \circ \tau^\beta.$$

Са $\alpha\beta$ означићемо композицију тј.

$$\tau^{\alpha\beta} = (\tau^\beta)^\alpha.$$

У односу на ове операције скуп k је тело изоморфно полазном телу K. Важи и следећа теорема [3]:

Теорема 11. *За $\alpha \in k$, $\alpha \neq 0$ и тачку P постоји јединствена дилатација σ са фиксном тачком P, за коју је*

$$\tau^\alpha = \sigma\tau\sigma^{-1}, \quad \textit{за свако} \quad \tau \in T. \qquad \square$$

Папусова теорема и закон комутативности

Показаће се да је у овом афином простору закон комутативности тела K еквивалентан са једном једноставном геометријском конфигурацијом.

За произвољну тачку $P \in \mathcal{A}$, елемент α тела k, на основу претходне теореме, можемо добити једном и само једном дилатацијом σ_α са фиксном тачком P. Тада је

$$\tau^\alpha = \sigma_\alpha \tau \sigma_\alpha^{-1}.$$

Ако је $\tau^\beta = \sigma_\beta \tau \sigma_\beta^{-1}$, онда је

$$\tau^{\alpha\beta} = (\tau^\beta)^\alpha = \sigma_\alpha\sigma_\beta\tau(\sigma_\alpha\sigma_\beta)^{-1},$$

док је с друге стране

$$\tau^{\alpha\beta} = \sigma_{\alpha\beta}\tau\sigma_{\alpha\beta}^{-1}.$$

Како је σ_α јединствено одређено са α, то је $\sigma_{\alpha\beta} = \sigma_\alpha\sigma_\beta$. То посебно значи да је мултипликативна група тела k изоморфна групи дилатација

са фиксном тачком P. Тело k (тиме и тело K) је комутативно акко је ова група дилатација комутативна.

Нека су сада l и m две различите праве кроз P и нека је Q произвољна тачка праве l различита од P. Ако је σ_1 дилатација којој је тачка P фиксна, онда је l σ_1-траг и тачка $\sigma(Q) = Q' \neq P$ биће тачка са праве l. Тиме је дилатација σ_1 у потпуности одређена. Аналогно тачкама R, R' праве m различитим од P, одређена је дилатација σ_2, којој је P фиксна тачка и $\sigma_2(R) = R'$.

Конструисаћемо тачке $S = \sigma_1\sigma_2(R) \in m$ и $T = \sigma_2\sigma_1(Q) \in l$. Оне су одређене следећим релацијама:

$$Q + R' \parallel \sigma_1(Q) + \sigma_1(R') = Q' + \sigma_1\sigma_2(R) = Q' + S,$$

$$R + Q' \parallel \sigma_2(R) + \sigma_2(Q') = R' + \sigma_2\sigma_1(Q) = R' + T.$$

Да би важила једнакост $\sigma_1\sigma_2 = \sigma_2\sigma_1$ потребно је и довољно да је $\sigma_1\sigma_2(Q) = \sigma_2\sigma_1(Q)$ или $\sigma_1\sigma_2(Q) = T$. Тачка $\sigma_1\sigma_2(Q)$ је на правој l, па је одређена релацијама:

$$Q + R \parallel \sigma_1\sigma_2(Q) + \sigma_1\sigma_2(R) = \sigma_1\sigma_2(Q) + S.$$

Из претходног је услов $Q+R \parallel T+S$ еквивалентан услову комутативности σ_1 и σ_2.

Занемаримо сада пресликавања σ_1 и σ_2. Тачка T праве l и тачка S праве m одређене су са

$$Q + R' \parallel Q' + S \quad \text{и} \quad Q' + R \parallel R' + T$$

и још захтевамо $Q + R \parallel T + S$. То јест, ако су бар два од три претходна пара паралелна, онда је и трећи. Ова конфигурација позната је као *Папусова* теорема. Из претходног следи:

Теорема 12. *Тело k је комутативно акко важи Папусова теорема.* □

Хармонијска спрегнутост

Пример 2. Свако инјективно пресликавање произвољне праве у афином простору $\mathcal{A}$ које чува хармонијску спрегнутост тачака је облика

$$\sigma(x) = ax^\tau + b,$$

где је $a \neq 0$, а τ је аутоморфизам или анти-аутоморфизам тела K. У доказу овог тврђења користи се теорема 1.6.8. [3]. ▽

2

ПРСТЕНИ КОСИХ ПОЛИНОМА

2.1 Појам прстена косих полинома

Прстен косих полинома је једно уопштење стандардног појма прстена полинома над комутативним прстеном. У овом уопштењу прстен коефицијената не мора бити комутативан и неодређена не комутира обавезно са коефицијентима. Посебно се задаје "закон комутирања", то јест прелазак неодређене с једне на другу страну коефицијената је "контролисан".

Нека је A произвољан прстен, S прстен који садржи A као свој потпрстен, као и фиксиран елемент t, $t \notin A$, такав да се сваки елемент прстена R генерисаног прстеном A и уоченим елементом t може на јединствен начин представити у облику

$$f = a_0 + ta_1 + \cdots + t^n a_n, \quad a_i \in A. \tag{1}$$

Овакав израз зваћемо *полиномом* по *неодређеној* t и његов *степен*, $\deg f$, дефинишемо са $\deg f = n$ ако је $a_n \neq 0$, док је нула полином степена $-\infty$. Ако је у (1) $a_n = 1$ за f кажемо да је *моничан*.

Услед дистрибутивности множења у R производ два елемента $f = \sum t^i a_i$ и $g = \sum t^j b_j$ је елемент $fg = \sum t^i (a_i t^j) b_j$. Да би и овај елемент записали у траженом облику уводимо правило по ком коефицијенти прелазе са леве на десну страну неодређене. Пре тога претпоставићемо још и да је:

$$\deg fg \leqslant \deg f + \deg g, \quad f, g \in R. \tag{2}$$

Услед тога је at за свако $a \in A$ степена највише 1, па за свако $a \in A$ постоје a^α, $a^\delta \in A$ за које је:

$$at = ta^\alpha + a^\delta, \quad a \in A. \tag{3}$$

Приметимо да су a^α и a^δ јединствено одређени елементом a, па су $a \mapsto a^\alpha$ и $a \mapsto a^\delta$ пресликавања прстена A у њега сама. Сада је задато множење у R, јер се индукцијом по $r \in \mathbb{N}$ може одредити и at^r за свако r :

$$at^r = (ta^\alpha + a^\delta)t^{r-1} = [t^2a^{\alpha^2} + t(a^{\alpha\delta} + a^{\delta\alpha}) + a^{\delta^2}]t^{r-2} = \dots \quad .$$

Изједначавањем израза:

$$(a+b)t = t(a+b)^\alpha + (a+b)^\delta \quad \text{и} \quad at + bt = ta^\alpha + a^\delta + tb^\alpha + b^\delta,$$

добијамо

$$(a+b)^\alpha = a^\alpha + b^\alpha, \quad (a+b)^\delta = a^\delta + b^\delta. \tag{4}$$

Аналогно из

$$(ab)t = t(ab)^\alpha + (ab)^\delta \quad \text{и} \quad a(bt) = a(tb^\alpha + b^\delta) = ta^\alpha b^\alpha + a^\delta b^\alpha + ab^\delta,$$

следи

$$(ab)^\alpha = a^\alpha b^\alpha, \quad (ab)^\delta = a^\delta b^\alpha + ab^\delta. \tag{5}$$

Даље, $1t = t1 = t$, и стога

$$1^\alpha = 1, \quad 1^\delta = 0. \tag{6}$$

Из (4) – (6) следи да је α ендоморфизам прстена A, а δ *α-деривација* прстена A, тј. пресликавање за које важи:

$$(a+b)^\delta = a^\delta + b^\delta, \quad (ab)^\delta = a^\delta b^\alpha + ab^\delta, \quad a, b \in A. \tag{7}$$

Обратно, ако је A произвољан прстен, α ендоморфизам и δ α-деривација прстена A, онда је скуп свих израза облика (1) прстен у односу на сабирање (сабирају се коефицијенти уз одговарајуће степене t^i) и множење дефинисано правилом (3). Провере су рутинске и показују да се у добијеном прстену сваки елеменат једнозначно изражава у облику (1). О томе говори и тврђење:

Тврђење 1. *Нека је A прстен, α ендоморфизам, δ α-деривација прстена A и $R = A\langle t;\ at = ta^\alpha + a^\delta,\ a \in A\rangle$. Тада важи:*

а) сваки $f \in R$ на јединствен начин може се приказати у облику (1),
б) ако је A домен и α инјективно онда је и R домен,
в) ако је A тело, онда је R десни главноидеалски домен; R је и леви главноидеалски домен ако је α аутоморфизам.

Доказ: Ако је A домен и α инјективно у (2) важи једнакост и стога је R домен. Даље, нека је A тело и I десни идеал у R. Уколико је $I = (0)$ тврђење важи. Иначе, нека је $p \in I$ моничан полином, $p \neq 0$, најмањег степена. Произвољно $f \in I$, користећи алгоритам дељења, видимо као $f = pq + r$, где $q, r \in R$ и $\deg r < \deg p$. Тада $r = f - pq \in I$, и ако је $r \neq 0$, у I постоји моничан полином степена строго мањег од степена p. Зато је $r = 0$ и тиме $f \in pR$. Значи $I = pR$, чиме је показано да је R десни главноидеалски. Ако је α аутоморфизам, и β његов инверз, за $a^\alpha = b$, (3) је облика $b^\beta t = tb + b^{\beta\delta}$ тј.

$$tb = b^\beta t - b^{\beta\delta}$$

одакле аналогно претходном следи да је R и леви главноидеалски домен.

□

Напомена. δ је *десна* α-деривација и неодређена је у (1) с'леве стране коефицијената. Аналогно се *левом* α-деривацијом (за коју важи: $(ab)^\delta = a^\alpha b^\delta + a^\delta b$) и захтевом да се сви елементи могу једнозначно записати у облику $a_0 + a_1 t + \cdots + a_n t^n$, $a_i \in A$ може конструисати симетричан појам.

Прстен R који смо претходно конструисали зваћемо *прстеном косих полинома* по неодређеној t над A који је индукован пресликавањима α и δ и означаваћемо га са $A[t;\alpha,\delta]$.

Дефиниција је уопштење класичне дефиниције прстена полинома, јер се за $\alpha = 1$ и $\delta = 0$ добија прстен полинома $A[t]$ са централном неодређеном t. Уколико је $\delta = 0$ уместо $A[t;\alpha,0]$ писаћемо само $A[t;\alpha]$. У складу са претходном напоменом прстен $A[t;\alpha,\delta]$ требало би звати левим прстеном косих полинома, да би нагласили да је неодређена са леве стране коефицијената. Прстен $A[t;\alpha,\delta]$ је и десни прстен косих полинома ако је α аутоморфизам.

Сваки инјективан ендоморфизам α десног Ореовог домена A може се на јединствен начин продужити до тела разломака K, и то једнакошћу $\alpha(ab^{-1}) = \alpha(a)(\alpha(b))^{-1}$. Исто важи и за α-деривације. Наиме, свака α-деривација δ индукује хомоморфизам

$$a \mapsto \begin{bmatrix} a & a^\delta \\ 0 & a^\alpha \end{bmatrix}$$

прстена A у прстен $T_2(A)$ горње троугаоних матрица над прстеном A. Овај хомоморфизам се услед функторијалности може продужити до хомоморфизма

$$u \mapsto \begin{bmatrix} u & u' \\ 0 & u^\alpha \end{bmatrix}$$

тела K у прстен $T_2(K)$. Пресликавање $u \mapsto u'$ је α-деривација на K која је продужење δ. Тиме смо показали да се свака деривација асоцирана инјективном ендоморфизму може продужити до K.

У наставку ћемо проучавати прстен косих полинома у облику у ком смо га првобитно задали, уз напомену да све што буде доказано, важи и за симетричан појам, уз одговарајућу промену формулације тврђења.

Прстен косих полинома над телом $K[t;\alpha,\delta]$ је главноидеалски здесна (сваки не нула ендоморфизам тела је инјективан), тиме и десни *Ореов*.

На основу 1.2. $K[t;\alpha,\delta]$ има и тело разломака, које ћемо означавати са $K(t;\alpha,\delta)$. Општије, нека је A десни *Ореов* домен са телом разломака K. Ако је α инјективан ендоморфизам и δ α-деривација прстена A, онда их можемо продужити до K. Тада важи:

$$A[t;\alpha,\delta] \subseteq K[t;\alpha,\delta] \subseteq K(t;\alpha,\delta).$$

Елементи $K(t;\alpha,\delta)$ су облика fg^{-1}, где $f,g \in K[t;\alpha,\delta]$. Ако је c заједнички десни садржалац именилаца коефицијената полинома f и g онда је $f = f_1 c^{-1}$ и $g = g_1 c^{-1}$ за одговарајуће $f_1, g_1 \in A[t;\alpha,\delta]$, $c \in A^\times$. Отуда је $fg^{-1} = f_1 g_1^{-1}$ што за последицу има:

Тврђење 2. *Прстен косих полинома над десним Ореовим доменом је и сам десни Ореов домен.* □

Следеће тврђење показаће да $K[t;\alpha,\delta]$ у општем случају не мора бити и леви Ореов.

Тврђење 3. *Нека је K тело са ендоморфизмом α и α-дериванцијом δ. У прстену $R = K[t;\alpha,\delta]$ следећи услови су еквивалентни:*

а) α је аутоморфизам,
б) R је главноидеалски слева,
в) R је леви Ореов.

Доказ: Да а)⇒ б) следи из тврђења 2.1.1., а а) ⇒ б) је очигледно. Да би доказали да в) ⇒ а) претпоставимо да важи в). Нека је $c \in K$. Како је R леви Ореов то постоје $f, g \in R$ за које је $ft = gtc \neq 0$. Из претходне једнакости следи $\deg f = \deg g$. Ако је $f = t^n a + \ldots$, а $g = t^n b + \ldots$ изједначавање коефицијената уз t^n даје $a^\alpha = b^\alpha c$. Отуда је $c = (b^{-1}a)^\alpha$, што показује да је α сурјективно, тиме и аутоморфизам. □

Нека су α и β ендоморфизми прстена A. Пресликавање $\delta : A \to A$ за које је:

$$(a+b)^\delta = a^\delta + b^\delta, \quad (ab)^\delta = a^\alpha b^\delta + a^\delta b^\beta, \quad a, b \in A$$

зваћемо (α,β)-*дериванцијом* прстена A. Специјално (α,β)-дериванције облика: $a \mapsto ca^\beta - a^\alpha c$ за $c \in A$ зваћемо *унутрашњим* (α,β)-*дериванцијама*. Дериванције које нису овог облика зваћемо *спољашњим*.

У прстену $R = A[t;\alpha,\delta]$ можемо извршити замену неодређене t новом $t' = ta + b$ за $a \in A^\times$ и $b \in A$. Тиме се R неће променити, али ће доћи до промене α и δ. Погодним заменама у појединим случајевима могуће је α редуковати на 1, а δ на 0.

Претпоставимо да је α *унутрашњи* аутоморфизам тј. $c^\alpha = ucu^{-1}$ за неко $u \in A^\times$. Заменом $t' = tu$, добијамо

$$ct' = ctu = (tc^\alpha + c^\delta)u = tuc + c^\delta u = t'c + c^\delta u, \ c \in A$$

чиме смо α свели на 1.

Претпоставимо сада да је δ *унутрашња* α-дериванција тј. $c^\delta = cd - dc^\alpha$ за неко $d \in A$. Заменом $t' = t - d$, добијамо

$$ct' = c(t-d) = tc^\alpha + c^\delta - cd = tc^\alpha - dc^\alpha = t'c^\alpha$$

чиме смо δ редуковали на 0.

Значи, уколико је бар једно од пресликавања α и δ унутрашње редукције су могуће. Уопште о овом проблему говори:

Теорема 4. *Нека је K тело са центром C и $R = K[t;\alpha,\delta]$ прстен косих полинома. Тада:*

а) ако је $\alpha(C) \neq C$, δ је могуће редуковати на 0,
б) ако је $\alpha(C) = C$, $\delta(C) \neq \{0\}$, α је могуће редуковати на 1,
в) ако је $\alpha(C) = C$, $\delta(C) = \{0\}$, онда је C садржан у центру прстена R.

Доказ: Претпоставимо да је $\alpha(C) \neq C$, тј. $\gamma^\alpha \neq \gamma$ за неко $\gamma \in C$. Заменом $t' = \gamma t - t\gamma$ за свако $c \in K$ је

$$ct' = c(\gamma t - t\gamma) = \gamma t c^\alpha + \gamma c^\delta - t c^\alpha \gamma - c^\delta \gamma = t' c^\alpha.$$

Тиме смо δ свели на 0. Даље, претпоставимо $\alpha(C) = C$ и да постоји $\gamma \in C$ за које је $\gamma^\delta \neq 0$. Онда је $\gamma^\alpha = \gamma$ и $\gamma c = c\gamma$ за свако $c \in K$ и отуда из $(c\gamma)^\delta = (\gamma c)^\delta$ следи

$$c\gamma^\delta + c^\delta \gamma = \gamma c^\delta + \gamma^\delta c^\alpha,$$

тј. $c\gamma^\delta = \gamma^\delta c^\alpha$. За $t' = t(\gamma^\delta)^{-1}$ је

$$ct' = tc^\alpha(\gamma^\delta)^{-1} + c^\delta(\gamma^\delta)^{-1} = t(\gamma^\delta)^{-1}c + c^\delta(\gamma^\delta)^{-1} = t'c + c^{\delta'},$$

где је δ' 1-деривација на K. У последњем случају α на C сводимо на 1, а δ на 0. Отуда t централизује C као и K, па је C садржан у центру прстена R. □

У специјалном случају када је $[K : C]$ коначан, сви C-линеарни ендоморфизми и деривације су унутрашњи, по Сколем-Нетериној теореми. Доказ ове теореме може се наћи у [8].

Тврђење 5. *Нека је K тело коначне димензије над својим центром C. Сваки C-линеарни ендоморфизам тела K је унутрашњи аутоморфизам и свака C-линеарна деривација је унутрашња.* □

Пример 1. Центар тела $\mathbb{H}$ реалних кватерниона једнак је $\mathbb{R}$. Стога је $\mathbb{H}$ коначне димензије над својим центром, па је по Сколем-Нетериној теореми сваки $\mathbb{R}$-линеарни ендоморфизам тела $\mathbb{H}$ унутрашњи, као и свака $\mathbb{R}$-линеарна деривација. Примера ради, ендоморфизам $\alpha(x) = -x$ тела $\mathbb{H}$ је $\mathbb{R}$-линеаран, тиме и унутрашњи. При том је $\alpha(x) = ixi^{-1}$.

Пример 2. Специјално свако поље је коначне димензије над својим центром, па је свака линеарна деривација унутрашња.

Сваком телу K можемо придружити тело разломака прстена $K[t]$ са централном неодређеном, $K(t)$. Центар овог тела описан је у следећем тврђењу:

Тврђење 6. *Нека је K тело са центром C. Центар тела $K(t)$ са централном неодређеном t једнак је $C(t)$.*

Доказ: Сваки елемент из $K(t)$ је облика $\varphi = fg^{-1}$ за неке $f, g \in K[t]$. Индукцијом по $d(\varphi) = \deg f + \deg g$ показаћемо да ако је φ у центру $K(t)$, да онда $\varphi \in C(t)$. Обрат је очигледан. Ако је $d(\varphi) = 0$, онда је $\varphi \in K$ и тврђење важи. Ако је $d(\varphi) > 0$, можемо претпоставити $\deg f \geqslant \deg g$, у супротном посматрамо φ^{-1} уместо φ. Користећи алгоритам дељења, $f = qg + r$, $\deg r < \deg g$ и $q, r \in K[t]$ су јединствено одређени. Нека је $u^c = c^{-1}uc$ за $u \in K(t), c \in K^\times$. Тада је

$$\varphi = fg^{-1} = q + rg^{-1}, \quad \varphi^c = q^c + r^c(g^c)^{-1}.$$

Како је φ у центру $K(t)$, $\varphi^c = \varphi$, тј.

$$q - q^c = r^c(g^c)^{-1} - rg^{-1}.$$

Са $v(\varphi) = \deg g - \deg f$ задата је валуација на $K(t)$. Лева страна претходне једнакости има валуацију $\leqslant 0$, осим ако је $q = q^c$, док десна страна има строго позитивну валуацију. Контрадикција! □

Пример 3. Како је центар тела реалних кватерниона $\mathbb{R}$, то је центар тела $\mathbb{H}(t)$ тело $\mathbb{R}(t)$. ▽

2.2 Примери прстена косих полинома

Пример 1. *Комплексни* прстен косих полинома $\mathbb{C}[t;-]$, као што смо видели, има за елементе полиноме са комплексним коефицијентима, а правило комутирања неодређене и коефицијената задато је са $at = t\bar{a}$.

Нека је $\mathbb{H}$ тело реалних кватерниона и f пресликавање

$$f : \mathbb{C}[t;-] \to \mathbb{H},$$

задато са $f(t) = j$. Тада је $f(1) = 1, f(i) = i, f(t) = j, f(t\bar{i}) = k$ и тиме $\operatorname{Im} f = \mathbb{H}$. Такође је $f(t^2+1) = 0$ тј. $t^2 + 1 \in \ker f$. Како ниједан полином нижег степена није у језгру и $\ker f$ је идеал у главноидеалском прстену $\mathbb{C}[t;-]$ (конјугација је аутоморфизам поља $\mathbb{C}$) то је $\ker f = (t^2+1)$. Сада је на основу теореме о изоморфизмима

$$\mathbb{C}[t;-]/(t^2+1) \cong \mathbb{H}.$$

Пример 2. Нека је $R = K(x)$ поље функција над пољем K. Извод $f \mapsto f'$ је 1-деривација на K. Тиме добијамо прстен $R[t;1,\prime]$ *диференцијалних оператора*. Уопште, нека је K тело са 1-деривацијом δ. Уколико је δ унутрашња, тј. $a^\delta = ac - ca$ за неко $c \in K$, у прстену $K[t;1,\delta]$ важи:

$$a(t-c) = ta + a^\delta - ac = (t-c)a, \quad a \in K.$$

Значи $x = t - c$ комутира са K и отуда $K[t;1,\delta] \cong K[x]$.

Нека је сада $K = K_0[x]$, где је K_0 тело и δ деривација на K дефинисана формалним диференцирањем по x (третирајући елементе из K_0 као константе):

$$(\sum x^i b_i)^\delta = \sum x^{i-1} i b_i.$$

Деривација δ није унутрашња (x у центру од K, а $x^\delta = 1$). Елементи $K[t;1,\delta]$ су облика $\sum t^i a_i(x)$, $a_i(x) \in K$ и још важи $xt = tx + x^\delta = tx + 1$. Отуда је

$$K[t;1,\delta] \cong \boldsymbol{A}_1(K_0),$$

где је $\boldsymbol{A}_1(K_0) = K_0\langle t, x\rangle/(tx - xt - 1)$ *Вејлова* алгебра. Вејлова алгебра је пример коначно генерисане, а бесконачнодимензионе алгебре која је за $\operatorname{char} K_0 \neq 0$ проста. Наиме, у сваком не нула идеалу можемо изабрати елемент $f(t,x)$ најнижег степена по t. Овај идеал садржаће и $df/dt = fx - xf$, који је нижег степена, па је стога једнак 0. То значи да је f полином само по x. Ако је његов степен по x најнижи, онда је $df/dx = tf - ft = 0$ и тиме $f = c \in K_0^\times$. То значи да сваки идеал садржи инвертибилан елемент, па је једнак целом прстену. Тиме је показано да је алгебра $\boldsymbol{A}_1(K_0)$ проста.

Пример 3. Нека је F поље карактеристике p и E/F сепарабилно раширење степена p, на пример $E = F(\xi)$, где $\xi^p - \xi \in F$. Пресликавање $\alpha : f(\xi) \mapsto f(\xi+1)$ је аутоморфизам поља E, реда p и $E[t;\alpha]$ је прстен косих полинома.

Пример 4. Нека је q степен простог броја p, $\boldsymbol{F}_q$ поље са q елемената и T ендоморфизам $f \mapsto f^q$ прстена $\boldsymbol{F}_q[x]$. Ако операцију множења са $a \in \boldsymbol{F}_q$ означимо са a, онда сваки полином $\sum T^i a_i$ дефинише један ендоморфизам прстена $\boldsymbol{F}_q[x]$. При том важи $aT = Ta^q$. Стога ендоморфизми чине прстен косих полинома $\boldsymbol{F}_q[T;\sigma]$, за $\sigma : a \mapsto a^q$. Претходно има примене у теорији коначних поља [20].

Пример 5. Нека је R домен са аутоморфизмом α. Локализацијом прстена $R[t;\alpha]$ по скупу $\{t^n : n \in \mathbb{N}\}$ добијамо прстен који ћемо означавати са $R[t,t^{-1};\alpha]$ и звати прстеном *косих Лорановиx полинома.*

Пример 6. Нека је K поље, $A = K[t]$ прстен полинома са централном неодређеном t. За $n = 2,3,\ldots$ пресликавања

$$\alpha_n : f(t) \mapsto f(t^n)$$

су ендоморфизми прстена A. Ниједан од њих није сурјективан, јер t не припада слици $\operatorname{Im}\alpha$. Нека је $R = A[x;\alpha_n]$ и S потпрстен прстена R генерисан са x и $y = xt$ над K. На основу тврђења 2.1.3. је $Sx \cap Sy = \{0\}$. Стога је подалгебра генерисана са x и y слободна. При том за свако $n \geqslant 2$ добијамо различите подалгебре и тиме неизоморфна утапања уочене слободне алгебре у тела, јер је:

$$x^{-1}yx = tx = xt^n = x(x^{-1}y)^n = (yx^{-1})^n x,$$

и тиме

$$x^{-1}y = (yx^{-1})^n.$$

Из претходног следи да слободна алгебра $K\langle x,y\rangle$ има више неизоморфних тела разломака, за разлику од комутативног случаја, где је тело разломака, уколико постоји јединствено одређено до на изоморфизам.

2.3 Структура идеала у прстенима косих полинома

Као што смо видели у претходним примерима неке алгебре изоморфне су количницима прстена косих полинима. Зато нам је од посебног интереса да одредимо елементе који генеришу двостране идеале. За елемент c прстена R рекли смо да је *инваријантан* ако је регуларан и $cR = Rc$.

Наредно тврђење даће опис двостраних идеала у доменима.

Тврђење 1. *Не нула идеал I домена R који је главни и као леви и као десни идеал генерисан је инваријантним елементом.*

Доказ: По претпоставци је $I = cR = Rc'$, тиме $c = uc', c' = cv$ тј. $c = uc' = ucv$. Сада $uc \in cR$, нпр. $uc = cw$ и отуда $cwv = ucv = c$, одакле је $wv = 1$.

Значи v је инвертибилан, па је $c'R = cvR = cR$ и тиме је c инваријантан генератор идеала I. □

Даље ћемо одредити моничне инваријантне елементе прстена полинома над телима са централном неодређеном. Тиме ћемо одредити и све инваријантне полиноме овог прстена, јер је сваки не нула полином асоциран са моничним.

Тврђење 2. *Нека је K тело са центром C и $K[t]$ прстен полинома над K са централном неодређеном t. Моничан полином прстена $K[t]$ је лево или десно инваријантан акко његови коефицијенти припадају C.*

Доказ: Очигледно сваки полином из $C[t]$ је и лево и десно инваријантан. Обратно, претпоставимо да је $f = t^n + t^{n-1}a_1 + \cdots + a_n$ десно инваријантан у $K[t]$. Тада је за свако $c \in K$, $cf = fc'$ за неко $c' \in K$ (изједначавањем степена у претходној једнакости). Из:

$$t^n c + t^{n-1}ca_1 + \cdots + ca_n = t^n c' + t^{n-1}a_1 c' + \cdots + a_n c'$$

следи $c = c', ca_i = a_i c'$ и отуда $ca_i = a_i c$, па $a_i \in C$ за све $i = 1, \ldots, n$. □

Пример 1. Моничан полином прстена $\mathbb{H}[t]$ је инваријантан акко припада $\mathbb{R}[t]$. ▽

У прстену $R = K[t; \alpha, \delta]$ над телом K сваки не нула идеал је облика fR за неки $f \neq 0$. При том је $Rf \subseteq fR$, па је f и десно инваријантан. Зато нам је од интереса да одредимо критеријум за десну инваријантност, и то моничних полинома. За $f \in K[t; \alpha, \delta]$ рећи ћемо да је *десно K-инваријантан* ако је $f \neq 0$ и $Kf \subseteq fK$. Приметимо да је f је десно инваријантан акко је десно K-инваријантан и $tf \in fR$. Тиме су довољни услови за десну инваријантност полинома $f = t^n + t^{n-1}a_1 + \cdots + a_n$: $cf = fc'$ за све $c \in K$ и $tf = f(tb + a)$ за $c', b, a \in K$. Заменом f у првом услову

$$cf = ct^n + \cdots = t^n c^{\alpha^n} + \ldots, \qquad fc' = t^n c' + \ldots$$

добијамо $c' = c^{\alpha^n}$. Слично је из другог услова

$$tf = t^{n+1} + t^n a_1 + \ldots,$$
$$f(tb + a) = t^{n+1}b + t^n a + t^{n-1}a_1 tb + \cdots = t^{n+1}b + t^n(a + a_1^{\alpha}b) + \ldots$$

$b = 1$, $a + a_1^{\alpha} = a_1$. Из претходног следи:

Тврђење 3. *У прстену $R = K[t; \alpha, \delta]$ над телом моничан полином f степена n је десно K-инваријантан акко је $cf = fc^{\alpha^n}$ за све $c \in K$; f је и десно инваријантан акко уз претходни услов важи $tf = f(t + a)$ за $a = a_1 - a_1^{\alpha}$, где је a_1 је коефицијент полинома f уз t^{n-1}.* □

Ако је α аутоморфизам тела K са инверзом β претходни услови еквивалентни су са $fc = c^{\beta^n}f$, $ft = (t - a^{\beta^n})f$, што значи да је f и лево инваријантан.

Последица 4. *Ако је у тврђењу 2.2.3. α аутоморфизам тела K, онда је сваки моничан десно (K-)инваријантан полином из R и (K-)инваријантан.* □

За моничан полином f из $K[t;\alpha,\delta]$ дефинишемо његову *дивергенцију*:

$$\Delta(f) = tf - f(t+a),$$

за $a = a_1 - a_1^{\alpha}$, где је a_1 коефицијент полинома f уз t^{n-1}. Приметимо да је $\deg \Delta(f) < \deg f$, јер се коефицијент уз t^n анулира.

Теорема 5. *Ако је f моничан десно K-инваријантан полином степена n у $R = K[t;\alpha,\delta]$ његова дивергенција $\Delta(f)$ је десно K-инваријантан полином степена мањег од n, а $\delta\alpha^n - \alpha^n\delta$ је унутрашња (α^n, α^{n+1})-деривација. Још, f је десно инваријантан акко је $\Delta(f) = 0$.*

Даље, ако је $u = \sum_{i=0}^{m} t^{m-i}a_i$ моничан десно K-инваријантан полином у R најмањег позитивног степена m, онда је

$$\Delta(u) = -a_m^{\delta} - a_m a, \text{ где је } a = a_1 - a_1^{\alpha},$$

u и је десно инваријантан уколико је α^{m+1} унутрашњи аутоморфизам.

Елемент u зваћемо *минималним* десно K-инваријантним елементом прстена R.

Доказ: За $c \in K$ и $\lambda = \alpha^n$ је:

$$\begin{aligned}\Delta(f) &= ctf - cf(t+a)\\ &= (tc^{\alpha} + c^{\delta})f - fc^{\lambda}(t+a)\\ &= tfc^{\alpha\lambda} + fc^{\delta\lambda} - ftc^{\lambda\alpha} - fc^{\lambda\delta} - fc^{\lambda}a\\ &= [tf - f(t+a)]c^{\alpha\lambda} + f[ac^{\alpha\lambda} + c^{\delta\lambda} - c^{\lambda\delta} - c^{\lambda}a].\end{aligned}$$

Отуда је:

$$c\Delta(f) - \Delta(f)c^{\alpha\lambda} = f[ac^{\alpha\lambda} + c^{\delta\lambda} - c^{\lambda\delta} - c^{\lambda}a].$$

Лева страна једнакости је степена $< n$, док десна страна има фактор степена n. Стога су обе стране једнакости 0. Тиме добијамо:

$$c\Delta(f) = \Delta(f)c^{\alpha^{n+1}}, \quad c^{\delta\lambda} - c^{\lambda\delta} = c^{\lambda}a - ac^{\lambda\alpha}.$$

Из претходног следи да је дивергенција $\Delta(f)$ десно K-инваријантна као и да је $\delta\lambda - \lambda\delta$ унутрашња (α^n, α^{n+1})-деривација.

Сада претпоставимо да је $u = \sum_{i=1}^{m} t^{m-i}a_i$ као у исказу теореме. С обзиром на то да је $\Delta(u)$ десно K-инваријантан и мањег степена то је $\deg \Delta(u) = 0$. У једнакости:

$$\Delta(u) = \sum t^{i+1}a_{m-i} - \sum t^i a_{m-i}t - \sum t^i a_{m-i}a,$$

слободан члан је $-a_m^{\delta} - a_m a$ и то је управо $\Delta(u)$. Уврштавањем у $c\Delta(u) = \Delta(u)c^{\alpha^{n+1}}$ добијамо или $\Delta(u) = 0$, тј. u десно инваријантан или $\Delta(u) \neq 0$, одакле следи да је α^{n+1} унутрашњи аутоморфизам. □

Помоћу претходне теореме извешћемо критеријум за испитивање простости прстена косих полинома.

Лема 6. *Ако прстен $K[t;\alpha,\delta]$ садржи десно K-инваријантан елемент позитивног степена, онда садржи и десно инваријантан елемент позитивног степена.*

Доказ: Доказаћемо прво да за моничне полиноме f и g при чему је g десно K-инваријантан важи

$$\triangle(fg) = \triangle(f)g + f\triangle(g).$$

Нека је $f = t^n + t^{n-1}a_1 + \ldots$ и $g = t^m + t^{m-1}b_1 + \ldots, a = a_1 - a_1^{\alpha}, b = b_1 - b_1^{\alpha}$, $\mu = \alpha^m$. Тада је $ag = ga^{\mu}$, па је

$$\begin{aligned}\triangle(f)g + f\triangle(g) &= [tf - f(t+a)]g + f[tg - g(t+b)] \\ &= tfg - f(t+a+g + ftg - fg(t+b) \\ &= tfg - fg(t+b+a^{\mu}).\end{aligned}$$

Како је $fg = t^{m+n} = t^{m+n-1}(b_1 + a_1^{\mu}) + \ldots$ то је претходно управо $\triangle(fg)$.

Нека је u минималан десно K-инваријантан елемент степена m. На основу теореме 2.2.5., $\triangle(u) \in K$. Применом претходно показаног за свако $n \geqslant 0$ је

$$\triangle(u^{n+1}) = \sum u^{n-i}\triangle(u)u^i = u^n(\sum_{i=0}^{n}\triangle(u)^{\alpha^{im}}).$$

При том $tu^{n+1} \in u^nR$ за све $n \geqslant 1$, одакле $t^su^n \in u^{n-s}R$, што је у uR за $s < n$. Како је $f = uq + r$, $degr < m$, то

$$fu^m = uqu^m + ru^m \in uR.$$

Тиме је $Ru^m \subseteq uR$ и uR садржи двострани идеал $Ru^mR \neq 0$ који је генерисан десним инваријантним елементом позитивног степена. □

Теорема 7. *Прстен $R = K[t;\alpha,\delta]$ је прост ако је (α^n, α^{n+1})-дериванија $\delta\alpha^n - \alpha^n\delta$ спољашња за свако $n \in \mathbb{N}$.*

Доказ: Ако R није прост, онда садржи неинвертибилан десно инваријантан елемент f. Ако је $degf = n$, по теореми 2.2.5. $\delta\alpha^n - \alpha^n\delta$ је унутрашња. Такође, по леми 2.2.6., ако је R прост, онда неће садржати ни неконстантне десно K-инваријантне елементе. □

Пример 2. Прстен диференцијалних оператора $R = \mathbb{R}(x)[t;1,\prime]$ је прост. На основу тврђења 2.3.3. моничан полином

$$f(t) = a_0(x) + ta_1(x) + \cdots + t^n, \quad a_i(x) \in \mathbb{R}(x)$$

је десно инваријантан у R акко је

$$tf(t) = f(t)(t + g(x)), \quad g(x) = a_{n-1}(x) - a_{n-1}(x)^{\alpha} = 0,$$

$$c(x)f(t) = f(t)c(x) \quad \text{за свако} \quad c(x) \in \mathbb{R}(x).$$

Други услов еквивалентан је са

$$t^nc(x) + t^{n-1}(nc'(x) + c(x)a_{n-1}(x)) + \cdots = t^nc(x) + t^{n-1}a_{n-1}(x)c(x) + \ldots$$

тј. са $c'(x) = 0$. Отуда други услов није испуњен ни за једнан моничан полином прстена R, што потврђује да је прстен R прост.

Приметимо да не важи обрат теореме 2.3.7.. Наиме у прстену R за свако $n > 0$ и свако $p(x) \in \mathbb{R}(x)$ је

$$p^{\delta\alpha^n - \alpha^n\delta} = 0.$$

Стога је $\delta\alpha^n - \alpha^n\delta$ унутрашња (α^n, α^{n+1})-деривација за свако $n > 0$, док као што смо видели прстен R је прост. ∇

Пример 3. Нека је k тело и K тело разломака слободног прстена $k\langle x_1, x_2, \ldots\rangle$ у ком неодређене комутирају; α, δ пресликавања тела K задата са $x_i^\alpha = x_{i+1}$, $x_i^\delta = x_{2i}$. Сада је

$$x_i^{\delta\alpha^n - \alpha^n\delta} = x_{2i+n} - x_{2(i+n)}.$$

За сваку унутрашњу (α^n, α^{n+1})-деривацију тела K је

$$x_i \mapsto cx_{i+n+1} - x_{i+n}c, \quad \text{за неко} \quad c \in K.$$

Упоређивањем са претходним изразом закључујемо да је за свако $n > 0$, $\delta\alpha^n - \alpha^n\delta$ није унутрашња (α^n, α^{n+1})-деривација. Сада из претходне теореме следи да је прстен $K[t; \alpha, \delta]$ прост. ∇

За аутоморфизам α тела K рећи ћемо да је *унутрашњег реда* r ако је r најмањи природан број за који је α^r унутрашњи, тј. облика $I(e) : a \mapsto eae^{-1}$. Ако је α^r спољашњи за све $r \in \mathbb{N}$ или α није аутоморфизам за α кажемо да је *бесконачног унутрашњег реда.*

Посебно ћемо размотрити случај када је $\delta = 0$.

Тврђење 8. *Нека је K тело са ендоморфизмом α и $R = K[t; \alpha]$.*

а) Ако је K бесконачног унутрашњег реда онда је сваки десно K-инваријантан елемент и десно инваријантан; десно инваријантни елементи су облика $t^r c$, $c \in K^\times$.

б) Ако је α аутоморфизам унутрашњег реда r нпр. $\alpha^r = I(e)$, онда $u = t^r c$ централизује K и инваријантни елементи су облика $t^m g$, где је g полином по u са коефицијентима у центру тела K.

Доказ: Нека је $f = t^n + t^{n-1}a_1 + \cdots + a_n$ десно инваријантан. Онда је $tf = f(t + a)$ за $a = a_1 - a_1^\alpha$. Изједначавањем коефицијената уз t^{n+1} следи $a = 0$. Сада је $tf = ft$ и тиме $a_i^\alpha = a_i$, $i = 1, \ldots, n$. Даље, за свако $c \in K$ важи $cf = fc^{\alpha^n}$ тј. $c^{\alpha^{n-i}}a_i = a_i c^{\alpha^n}$. Скраћивањем α^{n-i} (α^{n-i} је инјективно) добијамо $ca_i = a_i c^{\alpha^i}$, $i = 1, \ldots, n$. Пошто је α бесконачног унутрашњег реда то је $a_i = 0$ за све i. Значи $f = t^n$, па су у овом случају једини инваријантни елементи $t^n c$, $c \in K$.

Нека је α унутрашњег реда r и $\alpha^r = I(e)$. За $u = t^r e$ и $c \in K$ је

$$cu = ct^r e = t^r c^{\alpha^r} e = t^r ece^{-1}e = uc,$$

па u централизује K. Ако је f десно инваријантан аналагно као у претходном случају је $ca_i = a_i^\alpha c$. Стога је $a_i = 0$, осим у случају када $r \mid i$. То значи да је $f = t^m g$, где је g полином по u. Полином g

је и инваријантан, тј. $cg = gc^{\mu}$ за неки аутоморфизам μ. Из последње једнакости је $\mu = id$ и тиме $cg = gc$. За $g = \sum u^{s-i}b_i$ из једнакости $0 = gc - cg = \sum u^{s-i}(cb_i - b_ic)$, следи да су сви коефицијенти b_i у центру тела K. Тиме је тврђење доказано, јер је сваки десно инваријантан елемент и инваријантан на основу последице 2.2.4.. □

Пример 4. У прстену $\mathbb{C}[t;-]$, аутоморфизам $z \mapsto \bar{z}$ је унутрашњег реда 2, па у њему t^2 централизује све елементе из $\mathbb{C}$, док су десно инваријантни елементи облика $t^m g(t^2)$ (коефицијенти g су из $\mathbb{C}$). Ово су управо и сви десно $\mathbb{C}$-инваријантни елементи. ▽

Пример 5. Нека је $K = \mathbb{Q}(x)$, $\alpha : f(x) \mapsto f(x^2)$ и $R = K[t;\alpha]$. Како α није аутоморфизам тела K, то је α бесконачног унутрашњег реда, па су десно инваријантни елементи овог прстена облика $t^r f(x)$ за неко $f(x) \in K^{\times}$. ▽

У наредном примеру показаћемо да појмови десне K-инваријантности и десне инваријантности нису еквивалентни, тј. да постоји прстен косих полинома над неким телом K и у њему неки полином који је десно K-инваријантан, а није десно инваријантан.

Пример 6. Нека је $K = \boldsymbol{F}_p$ и E коначно раширење тела K степена $k \geqslant 2$, са аутоморфизмом $\alpha : a \mapsto a^p$. Пресликавање α је унутрашњег реда k и при том је $\alpha^k = I(1)$. Према претходној теореми сви десно инваријантни елементи прстена $R = E[t;\alpha]$ су облика $t^m g(u)$, где је $u = t^k$ и полином g је са коефицијентима у $\boldsymbol{F}_p$. Тиме је сваки десно инваријантан полином степена $\geqslant k$. С друге стране полином t је десно E-инваријантан, јер је $ct = tc^{\alpha}$, за свако $c \in E$, који према претходном није и десно инваријантан. ▽

Сада ћемо укључити и деривацију, а захтеваћемо да је α аутоморфизам. За елемент прстена косих полинома рећи ћемо да је *K-централан* ако централизује K.

Теорема 9. *Нека је K тело са аутоморфизмом α и α-дериватијом δ и $R = K[t;\alpha,\delta]$. Ако R није прост онда садржи неинвертибилне десно K-инваријантне елементе и нека је u моничан, најмањег позитивног степена m међу њима. Тада је или*

а) α бесконачног унутрашњег реда и у том случају сваки K-инваријантан елемент је облика $u^r c, r \in \mathbb{N}, c \in K^{\times}$, или је
б) α коначног унутрашњег реда и елемент облика $u^s c$ је K-централан. Ако је $v = u^d e$ K-централан најмањег позитивног степена, онда је сваки K-инваријантан елемент облика $f = u^r f_1 c$, где је f_1 полином по v са коефицијентима у центру од K и c индукује аутоморфизам $\alpha^{n-rm}, n = \deg f$, $m = \deg u$.

Доказ: На основу леме 2.2.6. R није прост ако садржи неинвертибилне K-инваријантне елементе. Нека је u минималан моничан K-инваријантан степена m. Сваки моничан K-инваријантан елемент f може се представити у облику $f = uq + r$, где $q, r \in R$, $\deg r < m$. По тврђењу 2.2.3., $cu =$

uc^μ, где је $\mu = \alpha^m$ и ако је $\deg f = n$ за $\nu = \alpha^n$, $fc^\nu = cf = cuq + cr = uc^\mu + cr$, одакле је

$$u(qc^\nu - c^\mu q) = cr - rc^\nu. \tag{1}$$

Лева страна једнакости садржи фактор степена m док је десна степена строго мањег од m, па се обе стране анулирају, тј. $cr = rc^\nu$. Тиме је r K-инваријантан и $\deg r < m$ па $r \in K$. Из једнакости (1) и чињенице да је α аутоморфизам имамо:

$$cq = qc^{\alpha^{n-m}}.$$

Понављајући поступак на q индукцијом по $\deg f$ добијамо

$$f = u^s + u^{s-1}b_1 + \cdots + b_s, \text{ где } b_i \in K. \tag{2}$$

Коефицијент уз u^s је 1, јер су и u и f монични. Још је и $n = sm$. Сада за свако $c \in K$ имамо:

$$fc^\nu = u^s c^\nu + u^{s-1}b_1 c^\nu + \cdots + b_s c^\nu,$$

$$cf = u^s c^{\mu^s} + u^{s-1}c^{\mu s-1}b_1 + \cdots + cb_s.$$

Изједначавањем добијамо $\nu = \mu^s$ и $cb_i = b_i c^{\mu^i}, i = 1, \ldots, s$.

Претпоставимо прво да је α бесконачног унутрашњег реда. Тада је $b_i = 0$ па је на основу (2) сваки K-инваријантан елемент облика $u^r c$, $c \in K$. Нека је сада α унутрашњег реда z. Тада је $\mu^i = \alpha^{im}$ унутрашњи акко $z \mid im$, па је $b_i = 0$ осим ако $z \mid im$. Стога је $f = u^s$ или $f = u^r g(u^d)$, где је $d = z/(z,m)$. По претпоставци је

$$cu^d = u^d c^{\alpha^{dm}} = u^d ece^{-1}$$

за неко $e \in K^\times$ и све $c \in K$. То значи да је $v = u^d e$ K-централан и $u^{-r}f$ може се записати као полином по v, нпр. $f = u^r(\sum v^j c_j)$. Сада је $h = u^{-r}f$ K-инваријантан степена $n - rm$. Ако је $\lambda = \alpha^{n-rm}$, онда је $ah = ha^\lambda$ и $0 = ah - ha^\lambda = \sum v^j(ac_j - c_j a^\lambda)$. Отуда је $ac_j = c_j a^\lambda$ и сви c-ови могу се добити из једног множењем елементом из центра K. Тиме је $f = u^r f_1 c$, где f_1 централизује K, а c индукује аутоморфизам α^{n-rm}. □

Применом претходног резултата одредићемо центар одговарајућег тела разломака (доказ [8]).

Теорема 10. *Нека је K тело са центром C. За задати аутоморфизам α и α-деривацију δ тела K посматрамо $U = K(t;\alpha,\delta)$ тело разломака прстена косих полинома $K[t;\alpha,\delta]$.*

а) Ако је R прост или је α бесконачног унутрашњег реда, онда је центар тела U скуп $C_0 = \{a \in C | a^\alpha = a, a^\delta = 0\}$

б) Ако R није прост и α је коначног унутрашњег реда, нека је v моничан инваријантан елемент најмањег позитивног степена који индукује унутрашњи аутоморфизам $I(c) : a \mapsto cac^{-1}$; тада је центар U управо $C_0(vc)$ тело рационалних функција по vc над C_0.

□

Пример 7. Прстен $R = \mathbb{C}[t;-]$ није прост, па применом другог дела претходне теореме можемо одредити центар тела $\mathbb{C}(t;-)$ и то је $C_0(t^2) = \mathbb{R}(t^2)$ с обзиром на то да је t^2 моничан инваријантан полином најмањег степена у R и да је $C_0 = \mathbb{R}$. ▽

Пример 8. Као што смо видели у примеру 2.3.2. прстен $K[t;1,\prime]$ је за $K = \mathbb{R}(x)$ прост, па је отуда центар тела $K(t;1,\prime)$ скуп

$$C_0 = \{a(x) \in C(x) \mid a(x)' = 0\} = \mathbb{R}.$$

▽

2.4 Прстени косих формалних степених редова

У комутативном случају прстен $K[[t]]$ можемо добити комплетирањем прстена $K[t]$ у односу на топологију у којој степени идеала (t) чине околинску базу нуле. Овај концепт можемо применити и на прстен $K[t;\alpha]$ за сваки ендоморфизам α прстена K. Тако добијамо прстен $K[[t;\alpha]]$ косих степених редова.

Посматрајмо прстен $K((t;\alpha))$ *косих Лоранових редова*. То су редови облика $\sum_{-r}^{\infty} t^i a_i$ које множимо користећи правило $at^n = t^n a^{\alpha^n}$. Како n може бити негативно, претпоставићемо да је α аутоморфизам. Приметимо да је $K((t;\alpha))$ тело, јер сваки ненула ред можемо представити у облику $t^{-r}c(1-\sum_1^{\infty} t^i a_i)$, па је његов инверз облика $[\sum_n(\sum_i t^i a_i)^n]c^{-1}t^r$. Тело косих Лоранових редова можемо конструисати и у случају када α није аутоморфизам и то локализацијом по скупу $\{1,t,t^2,\dots\}$. Међутим у овом случају, његови елементи не могу се представити у облику $\sum t^i a_i$.

Претпоставимо сада да је K тело са ендоморфизмом α и α-деривацијом δ. У овом случају за $\delta \neq 0$, множење више није непрекидна функција у односу на t-адичну топологију. То показује формула

$$at = t^\alpha + a^\delta, \tag{1}$$

па се комплетирање не може конструисати директно. Један начин да избегнемо овај проблем је да уведемо смену $z = t^{-1}$ и да правило (1) запишемо у функцији од z:

$$za = a^\alpha z + za^\delta z. \tag{2}$$

Узастопном применом (2) добијамо:

$$\begin{aligned} za &= a^\alpha + a^{\delta\alpha}z^2 + za^{\delta^2}z^2 = \dots \\ &= a^\alpha + a^{\delta\alpha}z^2 + a^{\delta^2\alpha}z^3 + \cdots + a^{\delta^{n-1}\alpha}z^n + za^{\delta^n}z^n. \end{aligned}$$

У случају прстена степених редова, претходни поступак можемо применити неограничен број пута и отуда:

$$za = a^\alpha + a^{\delta\alpha}z^2 + a^{\delta^2\alpha}z^3 + \dots. \tag{3}$$

Овако добијен прстен је домен, у ком је скуп $\{1,z,z^2,\dots\}$ леви Ореов. Даље можемо формирати прстен разломака са имениоцима у уоченом Ореовом скупу. То ће заправо бити прстен косих Лоранових редова по z:

Теорема 1. *Нека је K тело са ендоморфизмом α и α-дериваџијом δ; R прстен задат са:*

$$R = K\langle z; za = a^{\alpha}z + za^{\delta}z \text{ за свако } a \in K\rangle. \tag{4}$$

Прстен R има комплетираље $\widehat{R}$, које за елементе има степене редове $\sum a_i z^i$. Скуп $Z = \{1, z, z^2, \ldots\}$ је леви Ореов у R и његовим инвертоваљем добијамо тело које се састоји од степених редова облика:

$$\sum_{i=0}^{\infty} z^{-r} a_i z^i. \tag{5}$$

Уколико је α аутоморфизам ови редови су облика $\sum b_i z^i$ као и $\sum z^i c_i$.

Доказ: Посматрамо комплетираље $\widehat{R}$ које се састоји од редова облика $\sum_0^{\infty} a_i z^i$. Ови редови чине прстен у односу на множеље задато са (3). Обзиром да је α инјективно $\widehat{R}$ је домен. Из једнакости (3) следи да за свако $a \in K$ постоји $f \in \widehat{R}$ за који је $za = fz$. То значи да је z лево инваријантан. Стога је $zg = g^{\lambda}z$ за свако $g \in \widehat{R}$ и тиме $z^r g = g^{\lambda^r} z^r$. Овим је показано и да је скуп Z леви Ореов. Отуда елементи облика $z^{-r}f$ за $r \geqslant 0$ и $f \in \widehat{R}$ формирају прстен. За $f = \sum a_i z^i$ и $a_i \neq 0$, имамо

$$a_0^{-1} f = 1 - \sum b_i z^i, \text{ за } b_i = -a_0^{-1} a_i \ (i > 0).$$

Отуда је

$$f^{-1} = (1 - \sum b_i z^i)^{-1} a_0^{-1} = \sum_0^{\infty} (\sum b_i z^i)^n a_0^{-1}.$$

Претходни израз је такође облика $\sum c_i z^i$. Наиме за свако m, терми који се појављују у $(\sum b_i z^i)^n$ за $n > m$ не садрже z^m. Тиме је показано да је f инвертибилан.

Сада сваки ненула ред (5) можемо записати у облику $z^{-r} g z^s$, при чему су $r, s \geqslant 0$, а g је инвертибилан. Његов инверз је облика $z^{-s} g^{-1} z^r$. То значи да је локализација $\widehat{R}$ по скупу Z тело.

Ако је α аутоморфизам коефицијенте a_i у (5) можемо пребацити и на леву и на десну страну. Тиме смо показали да важи и последњи део теореме. □

За тело K са центром C, ендоморфизмом α и α дериваџијом δ подтело

$$C_0 = \{a \in C : a^{\alpha} = 0, a^{\delta} = 0\} \tag{6}$$

зваћемо (α, δ)-*редукованим центром* тела K.

Тврђење 2. *Нека је K тело са аутоморфизмом α бесконачног унутрашњег реда и α-дериваџијом δ. Ако је $\widehat{R}$ комплетираље прстена (4) и U његово тело разломака, онда је центар тела U (α, δ)-редуковани центар C_0 тела K.*

Доказ: Очигледно је $C_0 \subseteq C(U)$. Нека је $f = \sum a_i z^i \in U$. Ако је $cf = fc$, онда је $\sum(ca_i - a_i c^{\alpha^i})z^i = 0$, тј. $ca_i = a_i c^{\alpha^i}$. Отуда је $a_i = 0$ за свако $i > 0$ и $a_0 \in C$. Даље, a_0 централизује z уколико је

$$a_0 z^{-1} = z^{-1} a_0 = z^{-1} a_0^{\alpha} + a_0^{\delta},$$

тј. $a_0^{\alpha} = a_0$, $a_0^{\delta} = 0$, па $a_0 \in C_0$, што је и требало показати. □

Применом претходног добијамо критеријум рационалности аналоган оном у теорији комплексних степених редова.

Тврђење 3. *Критеријум рационалности*
Нека је K тело са аутоморфизмом α. Формални степени ред $\sum t^i a_i$ у $K((t;\alpha))$ је рационална функција по t акко постоје $r, n_0 \in \mathbb{N}$ и елементи $c_1, \ldots, c_r \in K$ за које је

$$a_n = a_{n-1}^{\alpha} c_1 + a_{n-2}^{\alpha^2} + \cdots + a_{n-r}^{\alpha^r} c_r \quad \textit{за све} \quad n > n_0. \tag{7}$$

Овај услов заправо значи да је $(\sum t^i a_i)(1 - \sum_1^r t^j c_j)$ полином осим ако изузмемо факторе t^{-k}. □

Ово поглавље завршићемо презентовањем две конструкције. Прва се односи на конструкцију спољашњих аутоморфизама.

Тврђење 4. *Нека је K поље са аутоморфизмом α, $E = K((t;\alpha))$, β аутоморфизам поља K који комутира са α и који је продужен до E коришћењем правила $t^{\beta} = t$. Тада је β унутрашњи аутоморфизам тела E акко је $\beta = \alpha^r$ за неко $r \in \mathbb{Z}$.*

Доказ: Ако је β унутрашњи аутоморфизам тела E, онда постоји $a \in E^{\times}$ за које је $u^{\beta} = a^{-1}ua$ за све $u \in E$, тј. $ua = au^{\beta}$. Нека је $a = \sum t^i a_i$. Како је $t^{\beta} = t$ то је

$$\sum t^{i+1} a_i = \sum t^i a_i t = \sum t^{i+1} a_i^{\alpha},$$

и отуда $a_i^{\alpha} = a_i$. За $u = b \in K^{\times}$ је $b(\sum t^i a_i) = \sum t^i a_i b^{\beta}$ тј. $\sum t^i (b^{\alpha^i} - b^{\beta}) a_i = 0$. Тиме је $b^{\beta} = b^{\alpha^i}$ кад год је $a_i \neq 0$. Претходно важи за неко i, па је $\beta = \alpha^r$ за неко $r \in \mathbb{Z}$. Обратно, ако је $\beta = \alpha^r$, онда је β унутрашњи аутоморфизам индукован са t^r. □

Пример 1. За $K = F(s)$, где је F поље карактеристике 0, и $\alpha : s \mapsto s+1$, пресликавање $\beta : s \mapsto s+1/2$ је спољашњи аутоморфизам тела $E = K((t;\alpha))$. ▽

Друга примена односи се на конструкцију тела са унапред задатим центром.

Тврђење 5. *За задато поље K постоји тело D чији центар је K и које је бесконачне димензије над K.*

Доказ: Тело $K(t)$ проширимо кореновима једначине $x^{2^n} = t$ за $n = 1, 2, \ldots$ и добијено тело означимо са $E = K(t, t^{1/2}, t^{1/4}, \ldots)$. Пресликавање $\alpha : f(t) \mapsto f(t^2)$ је аутоморфизам тела E и његово фиксно тело је управо K. Наиме, сваки елемент $f \in E$ је рационална функција по t^{2^r} за неко $r \in \mathbb{Z}$. Уколико $f \notin K$, скуп могућих вредности за r је ограничен одозго.

Изаберимо највеће могуће r, за које f није рационална функција по $t^{2^{r+1}}$. Како је f^α једна таква функција, то је $f^\alpha \neq f$. Отуда је фиксно тело пресликавања α управо K.

Нека је сада $D = E((x;\alpha))$ тело косих Лоранових редова. Тврдимо да је K центар тела D. Сваки елемент из D је облика $f = \sum x^i a_i$, $a_i \in E$. Ако је f елемент центра тела D, онда из $xf = fx$ тј. $\sum x^{i+1} a_i = \sum x^{i+1} a_i^\alpha$ следи $a_i^\alpha = a_i$ и тиме $a_i \in K$. Даље,

$$\sum x^i a_i t = ft = tf = \sum x^i t^{2^i} a_i,$$

повлачи $a_i(t - t^{2^i}) = 0$ тј. $a_i = 0$ осим за $i = 0$. Отуда је $f = a_0 \in K$, што је и требало показати. Како су $1, t, t^2, \ldots$ линеарно независни над K то је D бесконачне димензије над K. □

Примедба. Нека је $F = K((t))$ тело рационалних функција са ендоморфизмом $\alpha : f(t) \mapsto f(t^2)$. Тело разломака $F(x;\alpha)$ прстена косих полинома $F[x;\alpha]$ је подтело тела D, претходно конструисаног. Из доказа следи да ово тело такође има центар изоморфан са K.

2.5 Мальцев-Нојманова конструкција

Прстени степених и Лоранових редова представљају специјалан случај конструкције која ће бити описана у овом поглављу. Она се односи на проблем утапања групног прстена у тело, тј. за које групе G је могуће групни прстен kG, где је k тело, утопити у тело. Неопходан услов је да је kG домен, а за то је неопходно да је G торзионо слободна. Јер, ако је $u \in G$ коначног реда n, онда је

$$(1-u)(1+u+u^2+\cdots+u^{n-1}) = 0. \tag{1}$$

Уколико је G комутативна, овај услов је и довољан:

Теорема 1. *Нека је G комутативна група и k поље. Групни прстен kG може се утопити у тело акко је G торзионо слободна.*

Доказ: Једнакост (1) показује да је услов потребан. Претпоставимо да је G торзионо слободна. Уколико њену операцију запишемо адитивно, можемо је посматрати и као $\mathbb{Z}$-модул и како је G торзионо слободна овај модул можемо утопити у $\mathbb{Q}$-модул тј. G видимо као векторски простор над $\mathbb{Q}$. Уочимо уређену базу овог простора. Котистећи лексикографско уређење коефицијената добијамо тотално уређење на G, које G чини уређеном групом. Користећи мултипликативне ознаке закључујемо да на G имамо тотално уређење са особином $s \leqslant s', t \leqslant t' \Rightarrow st \leqslant s't'$. Нека је

$$a = a_1 s_1 + \cdots + a_m s_m, \quad \text{где} \quad a_i \in k^\times,\ s_1 < s_2 < \cdots < s_m,$$

$$\text{и} \quad b = b_1 t_1 + \cdots + b_n t_n, \quad \text{где} \quad b_j \in k^\times,\ t_1 < t_2 < \cdots < b_n.$$

Онда је $ab = a_1 b_1 s_1 t_1 + \ldots$, где тачкице означавају терме $> s_1 t_1$, што показује да је $ab \neq 0$. Тиме је kG комутативан домен па се може утопити у тело. □

Претходни резултат може се уопштити на уређене некомутативне групе. Показаћемо да се за сваку тотално уређену групу G групни прстен kG може утопити у тело. Пре тога навешћемо неколико дефиниција и тврђења о уређеним скуповима неопходних за доказ ове теореме.

Уређен скуп је *добро уређен* ако сваки непразан подскуп има најмањи елемент. Сваки добро уређен скуп је и тотално уређен (применимо дефиницију на парове елемената). *Антиланцем* зваћемо скуп по паровима неупоредивих елемената. У наредној леми (доказ [8]) наводимо својства парцијално уређених скупова која ћемо касније користити.

Лема 2. *У парцијално уређеном скупу S следећи услови су еквивалентни.*

а) сваки бесконачан низ садржи бесконачан растући подниз тј. за задати низ (a_i) у S постоји низ (n') у $\mathbb{N}$ такав да $m' < n' \Rightarrow a_{m'} \leqslant a_{n'}$;
б) сваки нерастући низ (a_i), $a_i \not\leqslant a_j$ за $i < j$, је коначан;
в) сваки строго опадајући низ $a_1 > a_2 > \dots$ је коначан и сваки антиланац је коначан. □

Парцијално уређен скуп који задовољава неки од услова а)-в) претходне леме зваћемо *парцијално добро-уређеним* (ПДУ) скупом. У тотално уређеним скуповима ова дефиниција подудара се са дефиницијом доброг уређења. Подскуп ПДУ скупа је ПДУ, као и слика при пресликавању које је сагласно са уређењем. Исто важи и за унију два ПДУ. Такође је производ два ПДУ скупа S, T ПДУ у односу на уређење задато са

$$(s,t) \leqslant (s',t') \quad \text{акко је} \quad s \leqslant s' \quad \text{и} \quad t \leqslant t'.$$

Наиме сваки бесконачан низ у $S \times T$ садржи бесконачан подниз у коме су прве компоненте у растућем поретку, а овај низ опет садржи бесконачан подниз у коме су друге компоненте у растућем поретку, тако да важи а).

Дивизионим уређењем на моноиду M зваћемо парцијално уређење $' \leqslant'$ на M за које је:

(О.1) $s \leqslant s', t \leqslant t' \Rightarrow st \leqslant s't'$ за све $s,t,s',t' \in M$,
(О.2) $1 \leqslant s$ за све $s \in M$.

Уколико важе (О.1-2) у M, онда $st = 1$ повлачи $s = t = 1$, јер из $1 \leqslant t$ следи $s \leqslant st = 1$ и отуда $s = 1$ и $t = st = 1$. Наредна лема ([8]) даје услове под којима је моноид са ПДУ генераторним скупом и сам ПДУ.

Лема 3. *Нека је M моноид са дивизионим уређењем. Ако је M генерисан парцијално добро-уређеним скупом X, онда је M и сам парцијално добро-уређен.* □

За моноид M и поље k посматрамо k-простор функција k^M. Сваком $f \in k^M$ придружимо његов *носач*, дефинисан са

$$\mathcal{D}(f) = \{a \in M \mid f(a) \neq 0\}.$$

Функције са коначним носачем чине потпростор $k(M)$ k-просрора k^M. На $k(M)$ дефинишемо множење:

$$fg = h, \quad \text{где је} \quad h(c) = \sum_{ab=c} f(a)g(b). \tag{1}$$

Како су f, g са коначним носачем претходна сума је коначна. Једноставно се проверава да је $k(M)$ изоморфан моноидном прстену kM, па се могу идентификовати.

Елементе k^M можемо видети и као формалне редове $\sum af(a)$, али онда настаје проблем са множењем, обзиром да за задато c једначина $ab = c$ може имати бесконачно много решења. Зато претпоставимо да на M имамо дивизионо уређење и уочимо подскуп $k((M))$ скупа k^M који за елементе има функције са парцијално добро-уређеним носачем. Овај скуп је и прстен:

Теорема 4. *За моноид M и поље k скуп $k((M))$ свих редова са парцијално добро-уређеним носачем је k–алгебра и kM је њена подалгебра. Инвертибилни елементи ове алгебре су редови чији носач садржи* 1.

Доказ: Нека су $\sum af(a), \sum bg(b) \in k((M))$. Њихови носачи $\mathcal{D}(f), \mathcal{D}(g)$ су ПДУ. Носач суме $f + g$ је подскуп $\mathcal{D}(f) \cup \mathcal{D}(g)$, па је ПДУ. Посматрамо сада носач производа fg. За задато $c \in M$ посматрамо скуп свих парова $(a, b) \in \mathcal{D}(f) \times \mathcal{D}(g)$ за које је $ab = c$. Ако је овај скуп бесконачан, онда ПДУ скупа $\mathcal{D}(f)$ обезбеђује егзистенцију бесконачног подниза (a_i, b_i) за који је $a_1 < a_2 < \ldots$; отуда $b_1 > b_2 > \ldots$, па $\mathcal{D}(g)$ садржи бесконачан нерастући подниз, што је контрадикција. Тиме једначина $ab = c$ има коначно много решења. Скуп $\mathcal{D}(fg)$ је као слика $\mathcal{D}(f) \times \mathcal{D}(g)$ при пресликавању $(a, b) \mapsto ab$ ПДУ, и отуда $fg \in k((M))$. Провере асоцијативности и дистрибутивности су једноставне, па је $k((M))$ k–алгебра. Подалгебра $k((M))$ која се састоји од елемената са коначним носачем је управо kM.

Ако је $\sum af(a)$ инвертибилан, онда за неко $a \in \mathcal{D}(f)$ постоји b за које је $ab = 1$, и тиме $a = 1$. Обратно, нека је f ред чији носач садржи 1. Дељењем коефицијената можемо обезбедити да је ред f облика $1 - g$, где је $g = \sum tg(t)$ $(t > 1)$. Тврдимо да је $1 + g + g^2 + \cdots \in k((M))$. Моноид генерисан $\mathcal{D}(g)$ са дивизионим уређењем је ПДУ по леми 2.5.3.. Отуда је $\bigcup \mathcal{D}(g^n)$ ПДУ и ниједан елемент из M није елемент бесконачно много $\mathcal{D}(g^n)$, јер решења једначине $a_1 \ldots a_n = c$ чине антиланац у ПДУ скупу. Отуда је $\sum g^n$ добро дефинисан са ПДУ носачем, и то је управо инверз f. □

Нека је сада G *уређена група* тј. група са тоталним уређењем за које важи (О.1). Користећи теорему 2.5.4. показаћемо да се kG може утопити у тело.

Теорема 5. *За уређену групу G и поље k скуп $k((G))$, редова над k са добро уређеним носачем у G, је тело.*

Доказ: Подскуп $M = \{u \in G \mid u \geqslant 1\}$ групе G је моноид са дивизионим уређењем. По теореми 2.5.4. $R = k((M))$ је k-алгебра. Такође је и домен. Наиме у R важи $1 \neq 0$, па за $f \in R^\times$ дефинишемо његов ред $o(f)$ као најмањи елемент скупа $\mathcal{D}(f)$. Тада важи $o(fg) = o(f)o(g)$, одакле следи

да је производ два не нула елемента различит од нуле. Тврдимо да је M (леви и десни) Ореов скуп у R. Нека је $u \in M$ и $f \in R$. За сваки елемент $p \in \mathcal{D}(f)$ важи $p \geqslant 1$, и тиме $u^{-1}pu \geqslant u^{-1}u = 1$, па је $f_1 = u^{-1}fu \in R$ и $uf_1 = fu$. Овим је показано да је M десни Ореов скуп; M је и леви Ореов што се аналогно показује. За локализацију L прстена R по M важи $L \subseteq k((G))$. Овде заправо важи једнакост, јер за $f \in k((G)), f \neq 0$ за које је нпр. $o(f) = v$ је $v^{-1}f \in R$ и $o(v^{-1}f) = 1$. Отуда је $v^{-1}f$ инвертибилан у R, па је $f = v \cdot v^{-1}f$ инвертибилан у L. Из претходног следи да је L тело које се подудара са $k((G))$. □

Примедба. Приметимо да доказ претходне теореме пролази и за некомутативна тела.

Конструкција тела степених редова у овој теореми позната је као *Мальцев-Нојманова конструкција.* Примењује се на слободне групе с обзиром на то да се ове могу уредити. Нека је F слободна група на скупу X и нека је X' скуп који је у бијекцији са X. Дефинишемо пресликавање скупа F у скуп формалних степених редова $\mathbb{R}\langle\langle X'\rangle\rangle$ са:

$$x \mapsto 1 - x', \quad x^{-1} \mapsto \sum_{n=0}^{\infty} x'^n, \quad \text{где} \quad x \quad \text{одговара} \quad x'.$$

Ово пресликавање је утапање. Сада се $\mathbb{R}\langle\langle X'\rangle\rangle$ може тотално уредити тако што произвољно уређење на X' продужимо до лексикографског уређења на слободном моноиду генерисаном X' и до уређења на $\mathbb{R}\langle\langle X'\rangle\rangle$ одређеног коефицијентом уз најнижи терм.

Последица 6. *Групна алгебра сваке слободне групе G може се утопити у тело.* □

Примедба. Слободна k-алгебра $k\langle X\rangle$ над X може се утопити у kF, групну алгебру слободне алгебре над X, а ова се утапа у $k((F))$. Ако уместо групе F посматрамо слободну групу G дефинисану са $((u,v),(w,x)) = 1$ (где је $(x,y) = x^{-1}y^{-1}xy$), $k\langle X\rangle$ можемо утопити у kG уколико је card $X > 1$. Како се G може уредити то добијамо још једно утапање $k\langle X\rangle$ у тело које није изоморфно телу $k((F))$.

2.6 Итерирани прстени косих полинима

Као примену Мальцев-Нојманове конструкције издвајамо конструкцију једностраних главноидеалских домена. Као што смо видели прстен полинома над телом увек је главноидеалски домен. Овај услов је и неопходан тј. ако је прстен полинома главни, прстен коефицијената мора бити тело. Ово важи и у случају прстена косих полинома уколико је ендоморфизам прстена над којим је прстен косих полинома задат аутоморфизам, али не важи за ендоморфизме који нису сурјективни. Прецизне услове у вези са овом проблематиком први је формулисао Јатегаонакар[1969]:

Теорема 1. *За прстен A са ендоморфизмом α прстен $R = A[t;\alpha]$ је десни главноидеалски домен акко је A десно главноидеалски домен и α слика*

$A \setminus \{0\}$ *у* $A^\times$. *Ако је* α *аутоморфизам прстен* R *је десни главноидеалски акко је* A *тело.*

Доказ: Ако је R десно главни, онда је и A као потпрстен који је и хомоморфна слика прстена R (за $t = 0$). За свако $a \in A \setminus \{0\}$ имамо $aR + tR = cR$, где је c највећи заједнички леви фактор за a и t. Како је c фактор a то је $\deg c = 0$, па је $t = cf$, где је $\deg f = 1$. Нека је $f = td + e$. Сада је $t = ctd + ce = tc^\alpha d + ce$, одакле је $ce = 0$, $c^\alpha d = 1$, па је c^α јединица. Из $au + tv = c$ за $t = 0$ добијамо да је a асоциран са c, а тиме је a^α асоциран са c^α. Обзиром да је c^α јединица исто важи и за a^α.

Обратно, ако важе задати услови, R је домен. Нека је I десни идеал у R. Ако је $I = (0)$ доказ је завршен, иначе нека је $n = \min\{\deg(f) \mid f \in I \setminus \{0\}\}$. Водећи коефицијенти полинома степена n из I заједно са 0 чине десни идеал у A, који је по претпоставци главни, рецимо генерисан елементом a. Ако је $f = t^n a + \cdots \in I$, онда је $a^\alpha \in A^\times$ и отуда $ft = t^{n+1}a^\alpha + \ldots$ има инвертибилан водећи коефицијент. Значи I садржи моничан полином степена $n + 1$ и аналогно за све више степене. Отуда је $I = fR$, па је R десни главноидеалски домен. Последњи део тврђења следи из чињенице, да за аутоморфизам α тражени услов важи једино ако је $A \setminus \{0\} = A^\times$. □

Овај резултат указује да се под претходним претпоставкама конструкција прстена косих полинома може итерирати и да при том у сваком кораку добијамо десни главноидеалски прстен, што сугерише увођење следеће дефиниције.

J-косим прстеном полинома зваћемо прстен косих полинома $A[t; \alpha]$ такав да је α инјективно и да задовољава *Јатегаонакаров услов*:

(J.0) $A^\alpha \subseteq A^\times \cup \{0\}$.

Овај услов важи уколико је A тело, али ће од интереса бити други случајеви. Једноставно се проверава да уколико је A домен да је то и J-коси прстен косих полинома над A.

Нека је τ ординални број. Прстен R зовемо *J-прстеном типа* τ, ако R садржи ланац потпрстена R_λ ($\lambda < \tau$), за који је:

(J.1) $R_0 = R^\times \cup \{0\}$ (отуда је R_0 тело),
(J.2) $R_{\lambda+1}$ је J-коси прстен косих полинома над R_λ, за све $\lambda < \tau$,
(J.3) $R_\lambda = \bigcup_{\mu<\lambda} R_\mu$ за сваки ординал $\lambda \leqslant \tau$,
(J.4) $R_\tau = R$.

Експлицитно имамо $R_{\lambda+1} = R[t_\lambda; \alpha_\lambda]$ и из дефиниције следи да се сваки елемент $c \in R$ на јединствен начин може представити у облику:

$$c = \sum t_{\lambda_1} \ldots t_{\lambda_r} c_{\lambda_1 \ldots \lambda_r} \quad (c_{\lambda_1 \ldots \lambda_r} \in R_0, \lambda_1 \geqslant \cdots \geqslant \lambda_r). \tag{1}$$

Такође је $R_\lambda^\times = R_0^\times$ за свако λ, и отуда имамо:

Последица 2. *Сваки J-прстен (произвољног типа* τ*) је десни главноидеалски домен.* □

Прстени косих полинома над телима су коси J-прстени типа 1. Представићемо Јатегонаокарову конструкцију косог J-прстена произвољног типа τ засновану на Мальцев-Нојмановој конструкцији.

Да би добили облик (1) потребно нам је правило комутирања неодређених облика

$$t_\mu t_\lambda = t_\lambda u_{\mu\lambda} \quad (\mu < \lambda),$$

где је $u_{\mu\lambda}$ јединица у R_0. Општије, претходно мора да важи за све производе t-ова које можемо као у (1) узети у нормалној форми. Сада нам је потребна формула облика:

$$t_\mu t_{\lambda_1} \dots t_{\lambda_r} = t_{\lambda_1} \dots t_{\lambda_r} u_{\mu\lambda_1\dots\lambda_r} \quad (\lambda_1 \geqslant \dots \geqslant \lambda_r, \lambda_1 > \mu, r \geqslant 1). \tag{2}$$

Испоставиће се да је ово заправо довољно за тражену конструкцију. Нека је $T = \{t_\lambda\}$ $(\lambda < \tau)$ фамилија неодређених. Са F_T означимо слободну групу на T, а са E тело $k((F_T))$. Нека је K подтело тела E генерисано елементима

$$u_{\mu\lambda_1\dots\lambda_r} = (t_{\lambda_1} \dots t_{\lambda_r})^{-1} t_\mu t_{\lambda_1} \dots t_{\lambda_r} \quad (\lambda_1 \geqslant \dots \geqslant \lambda_r, \lambda_1 > \mu, r \geqslant 1), \tag{3}$$

као што је сугерисано у (2). Тада важи:

Лема 3. *Централизатор сваког t_ν у телу K је k.*

Доказ: Нека је G подгрупа групе $F = F_T$ генерисана елементима облика $(t_{\lambda_1} \dots t_{\lambda_r})^{-1} t_\mu t_{\lambda_1} \dots t_{\lambda_r}$. Сваки генератор је непарне дужине тако да можемо говорити о средњем фактору. Средњи елемент произвољног елемента групе G не можемо скраћивати. Стога сваки елемент у G почиње са t_λ^{-1}, а завршава се са t_μ. Такође $t_\nu^n \notin G$ за свако $n \neq 0$. Сваки $a \in K$ може се записати у облику $a = \sum u a_u$, где u пролази G, и свака конјугација у односу на t_ν слика K у K:

$$t_\nu^{-1} u_{\mu\lambda_1\dots\lambda_r} t_\nu = u_{\lambda_r\nu}^{-1} \dots u_{\lambda_i\nu}^{-1} u_{\mu\lambda_1\dots\lambda_{i-1}\nu} u_{\lambda_i\nu} \dots u_{\lambda_r\nu},$$

где је $\lambda_{i-1} \geqslant \nu > \lambda_i$. Сада t_ν комутира са свим t_ν^n у F, тако да конјугација у односу на t_ν фиксира 1, а све остале елементе помера у бесконачно много орбита. Свака од њих генерисана је једним елементом који је облика $t_\nu^{-n} g t_\nu^n$ за $n > 0$ и неко $g \in G$. Отуда једнакост $t_\nu^{-1} a t_\nu$ важи једино ако је $\mathcal{D}(a) = \{1\}$ и тиме $a = a_1$, што је и требало показати. □

Као што смо видели конјугација у односу на t_ν индукује ендоморфизам групе G који ћемо означавати са α_ν. За свако уређење на F или на G конјугација је сагласна са уређењем тако да се α_ν може проширити до ендоморфизма на K, који ћемо опет означити са α_ν. За свако $a \in K$ имамо

$$a t_\nu = t_\nu a^{\alpha_\nu}. \tag{4}$$

Нека је R потпрстен од $E = k((F))$ генерисан са K и свим $t_\nu (\nu < \tau)$. Користећи (4) закључујемо да је сваки елемент из R коначна сума облика:

$$\sum t_{\lambda_1} \dots t_{\lambda_r} a_{\lambda_1\dots\lambda_r}, \quad \text{где} \quad a_{\lambda_1\dots\lambda_r} \in K. \tag{5}$$

Уколико λ_i нису у растућем поретку, онда за неко $i = 1, 2, \dots, r-1$ имамо $\lambda_i < \lambda_{i+1} \geqslant \dots \lambda_r$. Користећи једнакост (2) t_{λ_i} можемо пребацити на десну страну. Понављањем овог процеса онолико пута колико је потребно добијамо $\lambda_1 \geqslant \dots \geqslant \lambda_r$ у сваком терму у (5). Сада тврдимо да је уз

ову допуну представљање елемената у облику (5) јединствено. Претпоставимо да у R имамо релацију

$$\sum t_{\lambda_1} \dots t_{\lambda_r} a_{\lambda_1 \dots \lambda_r} = 0, \quad \text{где} \quad a_{\lambda_1 \dots \lambda_r} \in K, \quad \lambda_1 \geqslant \dots \geqslant \lambda_r. \tag{6}$$

Ако је највећи индекс који се појављује у (6) λ, онда (6) можемо записати у облику $\sum t_\lambda^i c_i = 0$, где је сваки c_i полином по t_μ ($\mu < \lambda$). Конјугацијом са t_λ добијамо коефицијенте $c_i^{\alpha_i}$ који припадају K, тако да t_λ задовољава неку једначину над K. Нека је нпр.

$$t_\lambda^n + t_\lambda^{n-1} b_1 + \dots + b_n = 0, \quad \text{где} \quad b_i \in K, \tag{7}$$

једначина најнижег степена (> 0) коју задовољава t_λ. Конјуговањем са t_λ добијамо још једну једначину степена n за t_λ која се због јединствености подудара са (7). Отуда је $b_i^{\alpha_\lambda} = b_i$ за све $i = 1, \dots, n$, и по леми 2.6.3. $b_i \in k$, па је t_λ алгебарски над k. Ово је очигледно нетачно, што показује да су сви коефицијенти у (6) нуле. Тиме смо показали да је представљање (5) јединствено. То значи да додавањем једног по једног t-а на K добијамо J-коси прстен косих полинома у сваком кораку, па је R J-прстен типа τ чиме смо доказали:

Теорема 4. *За свако поље k и сваки ординал τ постоји J-прстен типа τ који је k-алгебра.* □

J-прстени типа најмање 2 имају бројна необична својства. Прво, у њима постоје елементи са факторизацијом произвољне дужине. Као што показује једнакост

$$t_2 = t_1^n t_2 u_{12}^{-n} \quad n = 1, 2, \dots$$

t_2 може имати произвољно много левих фактора, али не и десних. J-прстен типа τ је десни Нетерин. Уколико га локализујемо по скупу свих полинома којима је константни терм различит од нуле добијамо прстен P. Џејкобсонов радикал прстена P је идеал $\mathcal{J} = t_1 P$. За степене $\mathcal{J}$ дефинисане са $\mathcal{J}^{\lambda+1} = \mathcal{J}^\lambda \mathcal{J}$, $\mathcal{J}^\lambda = \bigcap_{\mu<\lambda} \mathcal{J}^\mu$ за ограничен ординал λ, важи $\mathcal{J}^\lambda \supseteq t_\lambda P$, одакле следи да је $\mathcal{J}^\lambda \neq 0$ за све $\lambda < \tau$.

Напомена. J-прстен типа 2 може се конструисати и на следећи начин. Нека је k поље са ендоморфизмом α, које садржи елемент t трансценденталан над k^α. Нека је K подтело тела функција $k(y)$ које садржи све рационалне функције облика f/g, где y не дели g. Продужимо α до K користећи $y^\alpha = t$, а затим формирамо прстен косих степених редова $R = K[[x; \alpha]]$. Добијени прстен R је J-прстен типа 2.

2.7 Псеудо-линеарне трансформације

Псеудо-линаерна пресликавања представљају уопштење стандардног појма линеарних пресликавања векторских простора. Наиме, за тело K са аутоморфизмом α и α-деривацијом δ, за пресликавање десног K-простора V, $L : V \to V$ кажемо да је *псеудо-линеарно* (у односу на (α, δ)), ако је:

$$L(x+y) = L(x) + L(y), \quad L(xa) = L(x)a^\alpha + xa^\delta \quad (x, y \in V, a \in K). \tag{1}$$

Ова дефиниција укључује линеарна пресликавања (за $\alpha = 1, \delta = 0$), *семилинеарна* пресликавања ($K = \mathbb{C}, \delta = 0$ и α је конјугација), као и *диференцијалне* трансформације ($K = F(t), \alpha = 1$ и $\delta = d/dt$).

Претпоставимо да је V коначно-димензиони десни K-простор и нека је $e = [e_1, \ldots, e_n]$ једна његова база. Ако су слике базних вектора задате са:

$$L(e_j) = \sum e_i a_{ij}, \quad \text{где} \quad a_{ij} \in K,$$

онда је слика произвољног вектора облика

$$L(\sum e_j \xi_j) = \sum (L(e_j)\xi_j^\alpha + e_j \xi_j^\delta) = \sum e_i (\sum a_{ij}\xi_j^\alpha + \xi_i^\delta).$$

За $A = [a_{ij}]$ и $\xi = (\xi_1, \ldots, \xi_n)^T$, имамо

$$L(\xi) = A\xi^\alpha + \xi^\delta. \tag{3}$$

Обратно, свака $n \times n$ матрица A над K дефинише једну псеудо-линеарну трансформацију L на V одређену са (3). Заменом базе e базом $e' = eP$, $P \in GL_n(K)$, за $L(e) = eA$ и $L(e') = e'B$ важи

$$ePB = L(eP) = L(e)P^\alpha + eP^\delta = e(AP^\alpha + P^\delta),$$

одакле добијамо

$$PB = AP^\alpha + P^\delta. \tag{4}$$

За матрице A, B за које важи релација (4) кажемо да су (α, δ)-*конјуговане*. Обзиром да су матрице псеудо-линеарног пресликавања у различитим базама (α, δ)-конјуговане циљ нам је да одредимо канонску форму задате матрице у односу на (α, δ)-конјугацију.

За $R = K[t; \alpha, \delta]$ простор V можемо видети и као десни R-модул за $(\sum t^i a_i) \cdot v = \sum L^i(v) a_i$. Користећи једнакости (1) добијамо да је на овај начин добро дефинисана спољна K-операција на простору V. Десна K-база e простора V је сада генератриса десног R-модула V која задовољава релације $\sum e_i(a_{ij} - \delta_{ij}t) = 0$, или у матричној форми

$$e(A - tE) = 0. \tag{5}$$

Овај скуп једнакости у потпуности одређује простор V. Користећи сада дијагоналну редукцију у R, закључујемо да постоје $P, Q \in GL_n(R)$ за које је

$$P(A - tE)Q = \operatorname{diag}(\lambda_1, \ldots, \lambda_n), \quad \lambda_{i-1} \mid\mid \lambda_i. \tag{6}$$

Полиноме λ_i зовемо *инваријантним факторима* матрице A. Као десни R-модул V је изоморфан са

$$R/\lambda_1 R \oplus \cdots \oplus R/\lambda_n R. \tag{7}$$

Приметимо да је $R/\lambda R = 0$ акко је λ константа и то различита од нуле, као и да је $R/\lambda R \cong R$ акко је $\lambda = 0$. Како је $\dim_K(R/\lambda R) = \deg \lambda$, то је $\sum \deg \lambda_i = n$.

Ако са C означимо центар тела K, елемент $c \in C$ за који је $A - cE$ сингуларна матрица, зовемо *централном сопственом вредношћу* матрице A.

Тврђење 1. *Свака $n \times n$ матрица над телом има највише n централних сопствених вредности.*

Доказ: Постоје инвертибилне матрице P, Q над $K[t]$ за које је

$$P^{-1}(A - tE)Q = \operatorname{diag}(f_1, \ldots, f_r, 0, \ldots, 0), \quad \text{где } f_i \in K[t].$$

Нуле полинома $f = f_1 \cdots f_r$ у C су једине тачке у C у којима ранг матрице $A - tE$ пада, а број ових тачака је $\leqslant \deg f = n$. □

Једнакост (7) показује да је V, до на изоморфизам, директна сума цикличних R-модула, који је и сам цикличан акко су му сви инваријантни фактори осим једног инвертибилни. У том случају псеудо-линеарну трансформацију L и матрицу A која је представља зовемо (α, δ)-*цикличним*. Користећи (6) добијамо следећу карактеризацију:

Тврђење 2. *Нека је K тело са аутоморфизмом α и α-деривацијом δ. Квадратна матрица A над K је (α, δ)-циклична акко је $A - tE$ слабо асоцирана над $K[t; \alpha, \delta]$ са 1×1 матрицом.* □

Свака (α, δ)-циклична псеудо-линеарна трансформација L има нормалну форму. Ако је v генератор десног R-модула V и $v_i = L^{i-1}(v)$, онда је V над K генерисан векторима $v_1, v_2, \ldots$. Нека је v_{r+1} први од њих за који је скуп $\{v_1, \ldots, v_r, v_{r+1}\}$ линеарно зависан над K, нпр:

$$v_{r+1} = v_1 a_1 + \cdots + v_r a_r, \qquad \text{где } a_i \in K. \tag{8}$$

Применом L на (8) добијамо $v_{r+2} = \sum v_{i+1} a_i^{\alpha} + \sum v_i a_i^{\delta}$, што показује да је v_{r+2} такође линеарна комбинација $v_1, \ldots, v_r$. Исто важи за све v_{r+k} $(k = 1, 2, \ldots)$, па како је V генерисан векторима v_i, то је $r = n$ и $[v_1, \ldots, v_n]$ је једна база простора V над K. У односу на ову базу матрица пресликавања L је:

$$\begin{bmatrix} 0 & 0 & 0 & \ldots & 0 & a_1 \\ 1 & 0 & 0 & \ldots & 0 & a_2 \\ 0 & 1 & 0 & \ldots & 0 & a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 0 & a_{n-1} \\ 0 & 0 & 0 & \ldots & 1 & a_n \end{bmatrix}. \tag{9}$$

Ову матрицу зовемо *пратећом матрицом* полинома

$$f = t^n - a_1 - ta_2 - \cdots - t^{n-1} a_n. \tag{10}$$

Приметимо да је матрица $tE - A$ слабо асоцирана са f, као и да једнакост (8) можемо записати у облику $f(L)(v) = 0$.

Из (7) следи да је свака квадратна матрица над K (α, δ)-конјугована дијагоналној суми матрица облика (9).

За псеудо-линеарне трансформације Кејли-Хамилтонова теорема неће важити. Наиме, ако је L псеудо-линеарна трансформација и V асоцирани R-модул, минимални полином L је генератор двостраног идеала у R који анулира V. Овај полином може бити 0 и у случају када је V коначне димензије над K. Заправо, L ће имати минимални полином акко

је његов последњи фактор у (7) ограничен. У том случају граница овог фактора је минимални полином, а за матрицу пресликавања L кажемо да је ограничена.

Пример 1. Матрица

$$\begin{bmatrix} i & 0 & 0 & \dots & 0 & 0 \\ 0 & i & 0 & \dots & 0 & \\ 0 & 0 & i & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & i & 0 \\ t^n-1 & t^n-1 & t^n-1 & \dots & t^n-1 & t^n+\dots+t+1 \end{bmatrix}$$

је ограничена у прстену $R = \mathbb{C}[t,-]$. Наиме, ова матрица се елементарним трансформацијама своди на матрицу

$$\operatorname{diag}(1,\dots,1,t^n+\dots+t+1).$$

При том је полином $t^n+\dots+t+1$ ограничен у прстену R, јер је леви фактор инваријантног полинома $t^{2n}-1$. ▽

Пример 2. Прстен $R = K[t;1,d/dt]$, где је $K = F(x)$ за неко тело F карактеристике 0, је прост, па су инвертибилне матрице једине које су ограничине. ▽

3

КОНАЧНА КОСА РАШИРЕЊА И ПРИМЕНЕ

3.1 Степен раширења

Нека је K тело и E K-прстен. Прстен E можемо посматрати као леви и као десни векторски простор над K. Одговарајуће димензије означаваћемо са

$$[E:K]_L \quad \text{и} \quad [E:K]_R.$$

Када је и E тело ове бројеве звaћемо *левим* и *десним степеном* раширења E над K. Код многих тела ова два броја се подударају али то није увек случај.

Као и у комутативном случају важи формула о производу степена која је последица следећег тврђења:

Тврђење 1. *Нека су $K \leqslant E$ тела и V десни E-модул. Тада су димензије V над E и K у следећем односу:*

$$[V:K] = [V:E][E:K]_R, \tag{1}$$

кад год је бар једна страна једнакости коначна.

Доказ: Као и у комутативном случају ако је $\{u_\lambda\}$ десна E-база модула V и $\{v_i\}$ десна K-база тела E, онда је $\{u_\lambda v_i\}$ десна K-база модула V. □

Код раширења коначног степена могуће је разликовати делитеље нуле и неинвертибилне елементе:

Тврђење 2. *Нека је K тело и A K-прстен коначног десног степена над K. Тада је сваки десно регуларан елемент A инвертибилан тј. ако је A домен, онда је и тело.*

Доказ: Нека је $a \in A$ десно регуларан. Пресликавање $\lambda_a : x \mapsto ax$ је инјективно и десно K-линеарно на коначодимензионом K-простору. Тиме је и сурјективно, па је $ab = 1$ за неко $b \in A$. Сада је b десно регуларан:

$bx = 0 \Rightarrow x = abx = 0$, па постоји $c \in A$ такав да је $bc = 1$. Како је $c = abc = a$ то је $ab = ba = 1$ тј. a је инвертибилан. □

Наводимо сада један важан случај када су леви и десни степени једнаки:

Теорема 3. *Нека је E централно коначно тело, тј. тело коначне димензије над својим центром. Тада су за свако подтело $K \leqslant E$ леви и десни степен раширења E над K једнаки.*

Доказ: Нека је C центар тела E. По претпоставци E је C-алгебра коначног степена и $A = KC = \{\sum x_i y_i |\ x_i \in K,\ y_i \in C\}$ је подалгебра. Ако A посматрамо као K-прстен можемо изабрати базу левог K-простора A која се састоји од елемената из C. То ће такође бити и десна K-база A и отуда је:

$$[A : K]_L = [A : K]_R. \tag{2}$$

Стога је A C-алгебра коначног степена и домен као подалгебра од E, па је A и тело. Из (1) имамо

$$[E : C] = [E : A]_L[A : C] = [E : A]_R[A : C].$$

Дељењем са $[A : C]$ који је коначан ($[E : C]$ коначан), а затим множењем са (2) и поновним коришћењем (1) добијамо $[E : K]_L = [E : K]_R$, што је и требало показати. □

Једна од последица претходног тврђења је да су леви и десни степени једнаки и када је подтело комутативно:

Тврђење 4. *Ако тело E садржи комутативно подтело K за које је степен $[E : K]_R$ коначан, онда је E централно коначно и $[E : K]_L = [E : K]_R$.*

Доказ: Нека је C центар тела E и F подтело од E генерисано са C и K. Подтело F је комутативно, садржи C и степен $[E : F]_R$ је коначан. Тензорски производ $E \otimes_C F$ је проста алгебра са центром F ([7]) и хомоморфизам

$$E \otimes_C F \to \mathrm{End}_F(E_F), \tag{3}$$

који $\sum u_i \otimes \alpha_i$ $(u_i \in E, \alpha_i \in F)$ слика у ендоморфизам $x \mapsto \sum u_i x \alpha_i$ је утапање ($E \otimes F$ проста алгебра). Ако је при том $[E : F]_R = n$, онда је десна страна у (3) управо $M_n(F)$. Отуда је

$$[E : C] = [E \otimes_C F : F] \leqslant [M_n(F) : F] = n^2.$$

Значи тело E је централно коначно па тврђење следи из теореме 3.1.3. □

Наредни пример показаће да се леви и десни степен раширења у општем случају не подударају.

Пример 1. Нека је k поље, $K = k(t)$ и $\alpha : f(t) \mapsto f(t^2)$ ендоморфизам тела K. Прстен $E = K[x; \alpha]/(x^2)$ је раширење тела K и то левог степена 3, а десног 2. Наиме $[1, x]$ је десна K-база, а $[1, x, xt]$ лева, прстена E. ▽

3.2 Галуаова раширења и једначине над телима

Нека је K тело и G група аутоморфизама тела K. Подтелу $E \leqslant K$ придружићемо подгрупу

$$E^* = \{\sigma \in G |\ x^\sigma = x \text{ за свако } x \in E\}$$

групе G. И обратно свакој подгрупи $H \leqslant G$ придружићемо подтело

$$H^* = \{x \in K |\ x^\sigma = x \text{ за свако } \sigma \in H\}$$

тела K. Ако је $E^{**} = E$, E^* ћемо звати *Галуаовом* групом и означавати са $\mathrm{Gal}(K/E)$, док ћемо K/E звати *Галуаовим* раширењем.

За елемент α раширења L тела K кажемо да је *десно алгебарски* над K ако су његови степени десно линеарно зависни над K, тј. ако је α *леви* корен једначине

$$f(t) = a_0 + ta_1 + \ldots + t^n a_n, \quad a_i \in K, \text{ и нису сви } 0. \tag{1}$$

Такође кажемо да је α *лева нула* полинома $f(t) = \sum t^i a_i$.

Циљ нам је да одредимо везу између левих нула полинома f и његових фактора. Са f_c означићемо елемент добијен заменом неодређене t у полиному f елементом c тела K, при чему коефицијенти остају здесна. Ако је $g = \sum t^j b_j$ неки други полином, онда је $fg = \sum t^{i+j} a_i b_j$. Ако претпоставимо да је $f_c \neq 0$ добијамо:

$$(fg)_c = \sum c^{i+j} a_i b_j = \sum c^j f_c b_j = f_c \sum (f_c^{-1} c^j f_c) b_j.$$

Отуда је $(fg)_c = f_c g(f_c^{-1} c f_c)$, кад год је $f_c \neq 0$. Применом претходног на $f = (t-c)q + r$ за $t = c$ добијамо да је $r = f_c$. Закључимо:

Тврђење 1. *Нека је K тело, $c \in K$ и $f \in K[t]$. Тада је $f_c = 0$ акко је $t - c$ леви фактор полинома f. Даље, за произвољне $f, g \in K[t]$ и $c \in K$ важи:*

$$(fg)_c = \begin{cases} 0 & \text{ако је } f_c = 0 \\ f_c g(f_c^{-1} c f_c) & \text{ако је } f_c \neq 0 \end{cases}$$

тј. леве нуле полинома fg су или леве нуле полинома f или конјугати левих нула полинома g. □

Даље ћемо извести критеријум за сличност линеарних фактора у $K[t]$ и то применом прстена косих полинома.

Тврђење 2. *Нека је K тело са ендоморфизмом α и α-дериванцијом δ и $R = K[t; \alpha, \delta]$. Полиноми $t - a$ и $t - a'$ су слични у прстену R акко је*

$$a' = c^{-1} a c^\alpha + c^{-1} c^\delta \quad \text{за неко } c \in K^\times. \tag{2}$$

Специјално, у $K[t]$, $t - a$ је сличан $t - a'$ акко је a' конјугат елемента a.

Доказ: Из тврђења 1.2.1. имамо да је $t - a$ сличан $t - a'$ акко постоји комаксимална релација

$$p(t - a') = (t - a)q, \tag{3}$$

за неке $p, q \in R$. Коришћењем алгоритма дељења за одговарајуће f, p можемо заменити са $p-(t-a)f$ који је степена 0, тако да можемо претпоставити да је $p = c \in K^\times$. Упоређивањем степена закључујемо да је у том случају и $q \in K^\times$. Сада релацију (3) можемо записати у облику:

$$tc^\alpha + c^\delta - ca' = tq - aq,$$

одакле је $q = c^\alpha$, $c^\delta - ca' = -aq$ и тиме $c' = ac^\alpha + c^\delta$, што даје (2). Обратно, када важи (2), важи и (3) за $p = c$ и $q = c^\alpha$. □

Значи, ако је a лева нула полинома f, онда је и лева нула полинома fg, за сваки полином g. Такође, ако је a лева нула f и g онда је и лева нула $f - g$. Стога полиноми из $K[t]$ којима је a лева нула чине десни идеал у $K[t]$, који је и језгро пресликавања $f(t) \mapsto f(a)$. Уколико је $a \in K$ овај идеал генерисан је са $t-a$. За десно алгебарске над K то је десни главни идеал генерисан моничним полиномом најмањег степена коме је a лева нула. Тај полином је јединствено одређен и зваћемо га *минималним полиномом* елемента a над K. У Галуаовим проширењима овај полином растављa се на линеарне факторе:

Теорема 3. *Нека је L/K Галуаово проширење и $G = \mathrm{Gal}(L/K)$. Ако је $a \in L$ десно алгебарски над K и μ_a његов минимални полином, онда је*

$$\mu_a = (t - a_1) \dots (t - a_n),$$

где су $a_1, \dots, a_n$ облика a^σ за $\sigma \in G$.

Доказ: Како је $t - a$ минималан полином елемента a над L то је

$$\mu_a = (t-a)f(t) \quad \text{за неко } f \in L[t].$$

За $\sigma \in G$ је $\mu_a(t) = (t-a^\sigma)f^\sigma(t)$ тако да сви $t-a^\sigma$ имају најмањи заједнички десни садржалац $p(t)$. Овај полином је и десни фактор μ_a, инваријантан у односу на G, па су му коефицијенти у K. Отуда је $p = \mu_a$. Нека је сада

$$\mu_a(t) = (t-a_1)(t-a_2)\dots(t-a_r)q = q'q'',$$

где је $a = a_1$, и сваки a_i је облика a^σ за неко $\sigma \in G$, а r је највеће могуће. Тврдимо да је $q'' = 1$. У супротном постоји a', конјугат од a у односу на G, такав да $t - a'$ није леви фактор q'. Како је a' лева нула полинома μ_a, то је $t - a'$ леви фактор полинома μ_a. Најмањи заједнички десни садржалац $t - a'$ и q' је облика

$$(t - a')p_1 = q'p_2.$$

Ово је десно копроста релација, па је p_2 сличан десном фактору $t - a'$, који није јединица. Тиме је p_2 облика $t - a_{r+1}$, где је a_{r+1} по леми 3.2.2. сличан са a'. Сада је μ_a заједнички десни садржалац $t - a'$ и q' и отуда

$$\mu_a = q'(t - a_{r+1})f,$$

што је у контрадикцији са избором r. □

Пошто је свака лева нула полинома $p = (t - a_1)\dots(t - a_n)$ конјугована са неком од $a_1, \dots, a_n$, добијамо уопштење познате теореме, која каже да једначина степена n, над произвољним пољем, не може имати више од n решења:

Последица 4. *Леве нуле полинома степена n елементи су највише n класа конјугације.* □

Пример 1. У телу $\mathbb{H}$ елементи i, j, k су нуле полинома $t^2+1 \in \mathbb{H}[t]$. Такође је и сваки конјугат ових елемената нула овог полинома. То значи да полином t^2+1 има бесконачно много нула над $\mathbb{H}$. Међутим, све оне су елементи једне класе конјугације. ∇

Други специјалан случај добијамо када су елементи G само унутрашњи аутоморфизми:

Последица 5. *Нека је K тело са центром C и f иредуцибилан полином над C. Тада су све леве нуле полинома f које су у K конјуговане.*

Доказ: Ако је G група свих унутрашњих аутоморфизама тела K, онда је њено фиксно поље управо C. Ако је α лева нула полинома f у K, онда је $t-\alpha$ леви фактор f. Услед иредуцибилности, f је и минимални полином за α над C, па тврђење следи из теореме 3.2.3. . □

Могуће је конструисати полином са унапред задатим левим нулама.

Тврђење 6. *За елементе $a_1, \ldots, a_n$ тела K који нису међусобно конјуговани постоји јединствен моничан полином степена n, са левим нулама $a_1, \ldots, a_n$.*

Доказ: Ако су f и g два монична полинома степена n са a-овима као левим нулама, онда је $\deg(f-g) < n$. На основу последице 3.2.4. је $f-g=0$. Отуда постоји највише један полином са траженим својством. Потребно је још показати да такав полином постоји и за то ћемо користити индукцију по n. Претпоставимо да је g моничан полином степена $n-1$ коме су $a_1, \ldots, a_{n-1}$ леве нуле. Опет по последици 3.2.4. је $g(a_n) \neq 0$, па је на основу 3.2.1. $g(t)(t - g(a_n^{-1})a_n g(a_n))$ моничан полином степена n са левим нулама $a_1, \ldots, a_n$. □

Као примену претходних тврђења доказаћемо теорему:

Теорема 7. *Свако некомутативно тело је бесконачно. Општије, у некомутативном телу, сваки елемент је садржан у бесконачном комутативном подтелу.*

Доказ: Нека је K тело са центром C, где је $C \neq K$ и $|C| = q < \infty$. За задато $a \in K \setminus C$ означимо са f минимални полином елемента a над C. Нека је нпр. $\deg f = r$. Пресликавање $x \mapsto x^q$ је аутоморфизам $C(a)$ над C, степена r. Отуда је по последици 3.2.5. a^q конјуговано са a, па постоји $b \in K^\times$ за који је

$$bab^{-1} = a^q, \tag{4}$$

и тиме $b^s a b^{-s} = a^{q^s}$. Како је $a^{q^r} = a$, то a комутира са b^r (али не и са b). Сада је $E = C(a, b^r)$ поље, а десни E-модул разапет над $1, b, \ldots, b^{r-1}$ је некомутативно раширење поља E степена r. Нека је

$$b^s + b^{s-1}\lambda_1 + \cdots + \lambda_s = 0, \quad \lambda_i \in E,\ s \leqslant r \tag{5}$$

једнакост најмањег степена коју b задовољава над E. Уколико је помножимо слева са a^{q^s} и од тога одузмемо десни умножак елементом a исте једнакости, добијамо:

$$b^{s-1}(a^q - a)\lambda_1 + \cdots + (a^{q^s} - a)\lambda_s = 0.$$

Како је ова једнакост нижег степена, сви коефицијенти се анулирају. Тј. за $s < r$ је $\lambda_1 = \cdots = \lambda_s = 0$, а једнакост (5) своди се на $b^s = 0$, што је контрадикција. Отуда је $s = r$ тако да је (5) облика $b^r - \lambda_r = 0$, па је $[E(b) : E] = r$.

Претпоставимо да постоје коначна некомутативна тела и нека је K најмање међу њима. Његов центар означимо са C. Сваки елемент из K над C генерише комутативно подтело које је садржано у максималном подтелу E тела K. Услед минималности тела K, E је комутативно подтело, па је облика $E = C(a)$ за неко $a \in K$. Наиме, ако је $[E : C] = r$ и b са истим својствима као у претходном пасусу, онда због максималности E, $b^r \in E$. Како $b \notin E$, то је $E(b) = K$, опет због максималности E. Из претходног следи $[K : E] = [E : C] = r$, одакле је $[K : C] = r^2$, чиме је показано да r не зависи од избора тела E. Значи, сва максимална подтела тела K имају исти број елемената и с обзиром на то да су комутативна, она су и изоморфна и свако је облика $C(a)$. При том је минимална једнакост коју a задовољава над C за сва ова тела истог облика. На основу последице 3.2.5. сва ова тела су конјугована у K, тако да се $K^\times$ може записати као унија свих конјугата правих подгрупа $K^\times$. Ово је у контрадикцији са чињеницом да се свака коначна група не може представити као унија својих правих подгрупа и њихових конјугата. Из претходног следи закључак да је свако некомутативно тело бесконачно (Ведербурнова теорема).

За крај, претпоставимо да је C коначно и да је a алгебарски над C, јер у осталим случајевима тврђење тривијално важи. Ако је a степена r над C, одредимо $b \in K$ које задовољава једнакост (4). Тада је $[C(a,b) : C(a,b^r)] = r$ и $C(a,b^r)$ је комутативно, док $C(a,b)$ није. Уколико би $C(a,b^r)$ било коначно, исто би важило и за $C(a,b)$, што је у контрадикцији са полазном претпоставком. Отуда $C(a,b^r)$ мора бити бесконачно, чиме је доказан и други део тврђења. □

Примедба. Како је свако коначно тело комутативно то ће у свакој афиној равни са коначно много тачака важити Папусова теорема.

Сада можемо формулисати и тврђење којим описујемо својства полинома који имају две или више конјугованих нула.

Теорема 8. *Ако полином над телом K има две различите леве нуле у истој класи конјугације тела K, онда их има бесконачно у тој класи.*

Доказ: Нека је $f = \sum t^i c_i$. Ако су a и $b^{-1}ab$ леве нуле полинома f, онда је $\sum a^i c_i = 0$ и $b^{-1} \sum a^i b c_i = \sum (b^{-1}ab)^i c_i = 0$. Стога је

$$\sum a^i (1 + \lambda b) c_i = 0$$

за свако $\lambda \in C_K(a)$-централизатора елемента a у K. Тиме су

$$(1 + \lambda b)^{-1} a (1 + \lambda b)$$

леве нуле полинома f, које су за свако $\lambda \in C_K(a)$ различите. Из

$$(1 + \lambda b)^{-1} a (1 + \lambda b) = (1 + \lambda' b)^{-1} a (1 + \lambda' b)$$

следи

$$(1+\lambda b)(1+\lambda' b)^{-1} = \mu \in C_K(a).$$

За $\mu \neq 1$ је $1+\lambda b = \mu + \mu\lambda' b$. Како је $\mu \neq 1$ то је $\mu\lambda' \neq \lambda$, па је $b = (\mu\lambda' - \lambda)^{-1}(1-\mu)$, што је у супротности са $b \notin C_K(a)$. Тиме је $\mu = 1$ и $\lambda' = \lambda$. По теореми 3.2.7. $C_K(a)$ је бесконачно, што значи да имамо бесконачно много левих нула конјугованих са a. □

3.3 Псеудо-линеарна раширења

У овом одељку описаћемо један специјалан случај раширења тела коначног степена и то почев од *квадратних раширења* L/K за која је $[L:K]_R = 2$. Тада је за свако $u \in L \setminus K$, пар $1, u$ десна K-база тела L. Тиме се сваки елемент из L на јединствен начин може представити у облику $ux+y$, за $x, y \in K$. Отуда је:

$$au = ua^\alpha + a^\delta \quad \text{за свако} \quad a \in K, \tag{1}$$

и

$$u^2 + u\lambda + \mu = 0, \quad \text{за неке} \quad \lambda, \mu \in K. \tag{2}$$

Елементи a^α, a^δ јединствено су одређени елементом a и аналогно као у 2.1. показује се да је α ендоморфизам, а δ α-деривација тела K. Структура тела L у потпуности је одређена са K и једнакостима (1), (2).

Обратно, нека је K тело са ендоморфизмом α и α-деривацијом δ. У прстену $R = K[t; \alpha, \delta]$ уочимо полином $f = t^2 + t\lambda + \mu$ за који је идеал fR двостран. Тада је $L = R/fR$ прстен десног степена 2 над K. Уколико једначина (2) нема решења у K L ће бити и тело.

Ако задржимо услов (1), а модификујемо услов (2) можемо добити раширења вишег степена.

С тим у вези дефинишемо појам *псеудо-линеарног* раширења десног степена n, са генератором u, као раширење L тела K са десном K-базом $1, u, \ldots, u^{n-1}$ у којем важи (1) и

$$u^n + u^{n-1}\lambda_1 + \cdots + u\lambda_{n-1} + \lambda_n = 0, \quad \text{за} \quad \lambda_i \in K. \tag{3}$$

Претходна разматрања показују да је свако квадратно раширење псеудо-линеарно, што не важи и за раширења вишег степена. Наредно тврђење даће нам формулу за рачунање левог степена произвољног псеудо-линеарног раширења:

Тврђење 1. *Нека је L/K псеудо-линеарно раширење десног степена n. Тада је:*

$$[L:K]_L = 1 + [K:K^\alpha]_L + [K:K^\alpha]_L^2 + \cdots + [K:K^\alpha]_L^{n-1}, \tag{4}$$

где је α асоцирани ендоморфизам. Посебно је

$$[L:K]_L \geqslant [L:K]_R. \tag{5}$$

Једнакост важи акко је α аутоморфизам тела K.

Доказ: За $L_0 = K$, $L_i = uL_{i-1} + K$ $(i \geqslant 1)$ је $L_i = K + uK + \cdots + u^iK$, па је

$$K = L_0 \subset L_1 \subset \cdots \subset L_{n-1} = L$$

ланац десних K-модула. Да би показали једнакост (4) довољно је показати да је сваки L_i десни K-модул и да је

$$[L_i : L_{i-1}]_L = [K : K^\alpha]_L^i. \tag{6}$$

Користећи псеудо-линеарност, индукцијом по i једноставно се показује да је L_i десни K-модул. Нека је сада $\{e_\lambda\}$ лева K^α-база за K. Тврдимо да елементи

$$u^i e_{\lambda_{i-1}}^{\alpha^{i-1}} \cdots e_{\lambda_1}^{\alpha} e_{\lambda_0}, \tag{7}$$

где $\lambda_0, \lambda_1, \ldots, \lambda_{n-1}$ пролазе индексни скуп $\{e_\lambda\}$, чине базу $L_i(\mathrm{mod}\ L_{i-1})$. За $c \in K$ имамо

$$c = \sum c_{\lambda_0}^{\alpha} e_{\lambda_0} = \sum c_{\lambda_0\lambda_1}^{\alpha^2} e_{\lambda_1}^{\alpha} e_{\lambda_0} = \cdots = \sum c_{\lambda_0\ldots\lambda_{i-1}}^{\alpha^i} e_{\lambda_{i-1}}^{\alpha^{i-1}} \cdots e_{\lambda_0}.$$

Отуда је

$$u^i c \equiv \sum u^i c_{\lambda_0\ldots\lambda_{i-1}}^{\alpha^i} e_{\lambda_{i-1}}^{\alpha^{i-1}} \cdots e_{\lambda_0} \equiv \sum c_{\lambda_0\ldots\lambda_{i-1}} u^i e_{\lambda_{i-1}}^{\alpha^{i-1}} \cdots e_{\lambda_0} \ (\mathrm{mod}\ L_{i-1}),$$

што значи да је $L_i(\mathrm{mod}\ L_{i-1})$ над K разапет над елементима (7). Треба још показати њихову независност. Претпоставимо да је

$$\sum c_{\lambda_0\ldots\lambda_{i-1}} u^i e_{\lambda_{i-1}}^{\alpha^{i-1}} \cdots e_{\lambda_0} \equiv 0 \ (\mathrm{mod}\ L_{i-1}).$$

Враћајући се уназад добијамо да су сви коефицијенти

$$c_{\lambda_0\ldots\lambda_{i-1}} = 0,$$

па су елементи (7) линеарно независни и чине базу $L_i(\mathrm{mod}\ L_{i-1})$. Отуда важи једнакост (6), а тиме и (4). Остатак тврђења последица је једнакости (4). □

Свако псеудо-линеарно проширење је облика R/fR, где је $R = K[t; \alpha, \delta]$, а f је десно инваријантан полином, који је иредуцибилан над K.

Ако је K коначне димензије над својим центром, могуће је упростити псеудо-линеарна проширења. Наиме, по тврђењу 2.1.5. α и δ су у том случају унутрашњи. Ако претпоставимо да је $c^\alpha = ece^{-1}$ и $c^\delta = cd - dc^\alpha$ за све $c \in K$, формула $cu = uc^\alpha + c^\delta$ је облика

$$cu = uece^{-1} + cd - dece^{-1}.$$

Из претходног за $u' = ue - de$, имамо

$$cu' = u'c.$$

Стога за тела која су коначне димензије над центром без умањења општости можемо претпоставити да је $\alpha = 1, \delta = 0$.

За проширење L/K кажемо да је *централно* ако је $L = K \otimes_C E$, где је C центар тела K, а E комутативно проширење од C. Псеудо-линеарно

раширење је централно уколико је асоцирани ендоморфизам 1, деривација 0 и ако је генерисано елементом који поништава моничну једначину са централним коефицијентима.

Дефинишемо још и *биномно* или *чисто* раширење као псеудо-линеарно раширење у којем генератор поништава једначину облика

$$u^n - \lambda = 0,$$

а степен α^n асоцираног ендоморфизма α је унутрашњи аутоморфизам индукован елементом λ. Испоставља се да се сва псеудо-линеарна раширења са нула деривацијом добијају помоћу претходна два.

Теорема 2. *Нека је K тело са ендоморфизмом α. Свако псеудо-линеарно раширење K са ендоморфизмом α и нула α-деривацијом је биномно раширење неког централног раширења.*

Доказ: Свако псеудо-линеарно раширење са нула деривацијом је облика R/fR, где је $R = K[t;\alpha]$, а $f \in R$ је десно инваријантан полином, иредуцибилан над K. Ако је α бесконачног унутрашњег реда, једини такав полином по тврђењу 2.2.8. је t, тако да немамо правих раширења. Ако је α унутрашњег реда r, нпр. $\alpha^r = I(e)$, онда $t^r e$ централизује K и опет по 2.2.8. сваки инваријантан иредуцибилан полином је полином по u са коефицијентима у центру. Нека је g један такав полином. Сада је $F = C[u]/(g)$ комутативно раширење центра C тела K, а $L = K \otimes_C F$ је централно раширење K. Полазно раширење је биномно раширење L (до L је α продужено релацијом $u^\alpha = ue^{-1}e^\alpha$), одређено једначином $x^r - ue^{-1} = 0$. □

Биномна псеудо-линеарна раширења са деривацијом различитом од нуле су примери псеудо-линеарних раширења са различитим десним и левим степеном раширења, од којих је један коначан, а други бесконачан [8].

Лема 3. *Нека је $n \in \mathbb{N}$ и ω примитивни n-ти корен 1. Ако су u, v неодређене над $\mathbb{Z}[\omega]$ такве да је*

$$vu = \omega uv, \tag{8}$$

онда је

$$(u+v)^n = u^n + v^n. \tag{9}$$

Ова формула важи и у телима чија карактеристика дели n за одговарајуће ω.

Доказ: Развијањем леве стране једнакости (9), добијамо суму у којој су сви терми производи u-ова и v-ова. Сваки терм f степена i по u, укључује и све терме добијене из f цикличним пермутацијама фактора. Померањем последњег фактора u или v на прво место добијамо $\omega^i f$ без обзира на то да ли је вршено померање u или v. Отуда за суму s_f, свих цикличних пермутација f, важи $s_f = \omega^i s_f$, одакле је $s_f = 0$ за све $0 < i < n$. Како је $(u+v)^n$ сума оваквих терма, једини терми који ће преживети су u^n и v^n, па (9) важи. Ако је карактеристика p, $n = p^r m$, где $p \nmid m$ и ω примитивни m-ти корен 1, једнакост $(u+v)^m = u^m + v^m$ аналогно као и у претходном случају важи. Како је $u^m v^m = v^m u^m$, добијамо (9). □

Сада ћемо описати једну класу биномних раширења.

Теорема 4. *Нека је $n \in \mathbb{N}$, E тело са ендоморфизмом α и примитивним n-тим кореном 1 нпр. ω, који је у центру C тела E и фиксиран у односу на α (ако карактеристика $p \mid n$, $n = p^r m, p \nmid m$, онда је ω примитивни m-ти корен 1); δ α-деривација тела E за коју је*

$$\delta\alpha = \omega\alpha\delta, \tag{10}$$

и $L = E(t; \alpha, \delta)$. Тада се α може продужити до ендоморфизма тела L (означимо га опет са α), релацијом:

$$t^\alpha = \omega t, \tag{11}$$

а δ до α-деривације L релацијом:

$$t^\delta = (1 - \omega)t^2. \tag{12}$$

У односу на ове дефиниције је

$$ct = tc^\alpha + c^\delta \quad \text{за све} \quad c \in L. \tag{13}$$

Даље, ако је $\beta = \alpha^n$ ендоморфизам тела L , $\varepsilon = \delta^n$ β-деривација и K подтело тела L генерисано над E елементом $u = t^n$, онда је

$$K = E(u; \beta, \varepsilon),$$

и L/K је биномно раширење десног степена n.

Доказ: Покажимо прво да ω припада и центру тела L. Како је $\omega^n = 1$, то је $0 = (\omega^n)^\delta = n\omega^{n-1}\omega^\delta$ одакле је $\omega^\delta = 0$. Аналогно и у телима карактеристике p. По претпоставци је $\omega^\alpha = \omega$, што даје $t\omega = \omega t$. Користећи (13), констатујемо да је са (11) задат ендоморфизам прстена $E[t; \alpha, \delta]$ који се може продужити до L обзиром да је α инјективно. Аналогно, δ прво продужимо до α-деривације на $E[t; \alpha, \delta]$, а затим до L. Пресликавања $\delta\alpha$ и $\omega\alpha\delta$ су на E једнака, што за последицу даје $t^{\delta\alpha} = t^{\omega\alpha\delta}$. Сада су ова пресликавања (α, α^2)-деривације које се слажу на генераторном скупу тела L, па су једнака.

Означимо са α_0 и δ_0 пресликавања α и δ на $E[t; \alpha, \delta]$ посматрана само на коефицијентима. Сада (13) можемо записати у облику

$$\rho(t) = \lambda(t)\alpha_0 + \delta_0,$$

где ρ и λ означавају десно и лево множење са t. Како је $\lambda(t)\alpha_0 = \alpha_0\lambda(t)$ и $\delta_0 \cdot \lambda(t)\alpha_0 = \omega\lambda(t)\alpha_0 \cdot \delta_0$, на основу леме 3.3.3. је

$$\rho(t^n) = \lambda(t^n)\alpha_0^n + \delta_0^n. \tag{14}$$

Из (11) следи да α^n фиксира t, па је $\alpha_0^n = \alpha^n = \beta$. Пресликавање ε тела L одређено са

$$ct^n = t^n c^\beta + c^\varepsilon, \tag{15}$$

је β-деривација која се на основу (14) слаже са δ_0^n на $E[t; \alpha, \delta]$, тиме и са δ^n. Сада је E-потпрстен тела L генерисан са t^n над E, облика $E[u; \beta, \varepsilon]$, где је $u = t^n$, па је подтело од L генерисано са t^n над E

облика $E(u;\beta,\varepsilon)$. Тврдимо да су $1,t,\ldots,t^{n-1}$ десно линеарно независни над K. Претпоставимо да у L важи релација $\sum_0^{n-1} t^i a_i = 0, (a_i \in K)$. Множењем заједничким имениоцем, следи да a_i могу бити полиноми по u и упоређивањем степена добијамо $a_i = 0$ за $i = 0,1,\ldots,n-1$. Да је L/K псеудо-линеарно довољно је проверити да су β и ε пресликавања скупа K у њега сама, што је последица чињеница: $u^\beta = u$ (11), за $u = t^n$ и $u^\varepsilon = 0$ (15). Коначно L/K је биномно раширење, јер је $t^n = u$. □

3.4 Квадратна раширења

Као што смо видели за свако $u \in L \setminus K$ једна база квадратног раширења L/K је $[1,u]$. Ово раширење је још одређено једнакостима

$$au = u^\alpha + a^\delta \quad \text{за свако} \quad a \in K, \tag{1}$$

$$u^2 + u\lambda + \mu = 0, \tag{2}$$

где $\lambda,\mu \in K$, α је ендоморфизам и δ α-деривација тела K.

Квадратна раширења могу се добити и као количници прстена косих полинома $R = K[t;\alpha,\delta]$ по идеалу облика fR, где је

$$f = t^2 + t\lambda + \mu, \tag{3}$$

$\lambda,\mu \in K$ акко је:

а) fR двострани идеал прстена R;

б) R/fR нема делитеља нуле.

Услов а) важи акко је f десно инваријантан, тј. ако $af \in fR$ за све $a \in K$ и $tf \in fR$. Користећи чињеницу да је сваки полном по t конгруентан (mod fR) тачно једном линеарном полиному директно ћемо извести услове потребне за валидност а). При том је:

$$\begin{aligned} af &= at^2 + at\lambda + a\mu \\ &= (ta^\alpha + a^\delta)(t+\lambda) + a\mu \\ &= t^2a^{\alpha^2} + ta^{\alpha\delta} + ta^{\delta\alpha} + a^{\delta^2} + ta^\alpha\lambda + a^\delta\lambda + a\mu \\ &\equiv t(a^{\alpha\delta} + a^{\delta\alpha} + a^\alpha\lambda - \lambda a^{\alpha^2}) + a^{\delta^2} + a^\delta\lambda + a\mu - \mu a^{\alpha^2} \pmod{fR}. \end{aligned}$$

Ако $ar \in fR$, коефицијенти на десној страни морају се анулирати и тиме добијамо:

$$a^{\alpha\delta} + a^{\delta\alpha} = \lambda a^{\alpha^2} - a^\alpha\lambda, \tag{4}$$

$$a^{\delta^2} + a^\delta\lambda = \mu a^{\alpha^2} - a\mu. \tag{5}$$

Приметимо да услов (4) значи да је $\alpha\delta+\delta\alpha$ унутрашња(α,α^2)-деривација. Слично (5) изражава чињеницу да је $\delta^2 + \delta\alpha$ унутрашња α^2-деривација индукована са μ. Даље, посматрамо $tf = t^3 + t^2\lambda + t\mu$ и

$$ft = t^3 + t^2\lambda^\alpha + t(\mu^\alpha + \lambda^\delta) + \mu^\delta;$$

за које је

$$\begin{aligned} tf &\equiv t^2(\lambda - \lambda^\alpha) + t(\mu - \mu^\alpha - \lambda^\delta) - \mu^\delta \pmod{fR}, \\ &\equiv t(\mu - \mu^\alpha - \lambda^\delta - \lambda(\lambda - \lambda^\alpha)) - \mu^\delta - \mu(\lambda - \lambda^\alpha) \pmod{fR}. \end{aligned}$$

Претходно је у fR ако су оба коефицијента 0:

$$\lambda^\delta = \mu - \mu^\alpha - \lambda(\lambda - \lambda^\alpha), \tag{6}$$

$$\mu^\delta = \mu(\lambda - \lambda^\alpha). \tag{7}$$

Закључак је да је f инваријантан ако важе једнакости (4) – (7).

Претпоставимо сада да су ове једнакости задовољене. Поставља се питање када је R/fR домен (тиме и тело)? Прстен R/fR има делитеље нуле акко постоје $a, b, c, d \in K$ за које је

$$(ta + b)(tc + d) \equiv 0 \pmod{fR},$$

а да су при том и (a, b) и (c, d) различити од $(0, 0)$. Ова конгруенција је могућа једино ако је лева страна степена 2 по t тј. и a и c су различити од нуле. У том случају b можемо заменити са $-ba$, а d са $-dc$, па дељењем са c добијамо:

$$(t - b)a(t - d) \equiv 0 \pmod{fR}.$$

У односу на (mod fR) имамо

$$\begin{aligned} (t-b)a(t-d) &= tat - bat - tad + bad \\ &= t^2a^\alpha + ta^\delta - t(ba)^\alpha - (ba)^\delta - tad + bad \\ &= t(a^\delta - (ba)^\alpha - ad - \lambda a^\alpha) + bad - (ba)^\delta - \mu a^\alpha. \end{aligned}$$

Изједначавањем коефицијената добијамо:

$$ad = a^\delta - (ba)^\alpha - \lambda a^\alpha. \tag{8}$$

$$bad = (ba)^\delta + \mu a^\alpha. \tag{9}$$

Заменом ad из (8) налазимо

$$b(a^\delta - (ba)^\alpha - \lambda a^\alpha) = (ba)^\delta + \mu a^\alpha.$$

Користећи сада да је $(ba)^\delta = b^\delta a^\alpha + ba^\delta$, претходно можемо упростити до

$$b^\delta a^\alpha + \mu a^\alpha + bb^\alpha a^\alpha + b\lambda a^\alpha = 0.$$

Како је $a \neq 0$, то је и $a^\alpha \neq 0$, па дељењем са a^α добијамо

$$bb^\alpha + b\lambda + b^\delta + \mu = 0. \tag{10}$$

Значи, ако прстен R/fR има делитеља нуле, онда једначина (10) има решења у K. Обратно, ако (10) има решење $b \in K$, за $a = 1$ и d одређено једнакошћу (8) добијамо да R/fR има делитеља нуле. Стога је егзистенција решења једначине (10) потребан и довољан услов за егзистенцију делитеља нуле у прстену R/fR.

Ако је L/K генерисано елементом u који задовољава (1) и (2), онда је такође генерисано и елементом $v = ua + b$, где $a, b \in K$ и $a \neq 0$. Правило комутирања за v добијамо заменом у (1):

$$\begin{aligned} cv = c(ua+b) &= uc^\alpha a + c^\delta a + cb \\ &= (v-b)a^{-1}c^\alpha a + c^\delta a + cb \\ &= va^{-1}c^\alpha a + c^\delta a - ba^{-1}c^\alpha a + cb. \end{aligned}$$

На овај начин α је промењено унутрашњим аутоморфизмом индукованим са a. Ако фиксирамо α за a можемо узети 1, а уместо c^δ сада имамо $c^\delta + cb - bc^\alpha$, тако да је у овом случају δ промењено унутрашњом α-деривацијом. Сумираћемо претходне резултате у теореми:

Теорема 1. 1) *Нека је L/K квадратно раширење. За сваки $u \in L \setminus K$ $[1, u]$ је десна K-база тела L и постоји ендоморфизам α тела K и α-деривацијом δ за које је*

$$au = ua^\alpha + a^\delta \text{ за све } a \in K,$$

и постоје $\lambda, \mu \in K$ за које је

$$u^2 + u\lambda + \mu = 0.$$

Ендоморфизам α одређен је до на унутрашњи аутоморфизам K, и за фиксирано α, δ је одређено до на унутрашњу α-деривацију тела K.

2) *За задато тело K са ендоморфизмом α и α-деривацијом δ постоји квадратно раширење тела K са десном базом $[1, u]$ за коју важе (1) и (2) акко је $\alpha\delta + \delta\alpha$ унутрашња (α, α^2)-деривација индукована са λ, $\delta^2 + \delta\alpha$ је унутрашња α^2 деривација индукована са μ, λ^δ и μ^δ задати су редом једнакостима (6) и (7) и K не садржи елемент b који задовољава једнакост (10).* □

Пример 1. Нека је $F = \mathbb{Q}(u)$, где је u одређен релацијом

$$u^2 + u + 2 = 0$$

и $\sigma : u \mapsto u^2$ $\mathbb{Q}$-аутоморфизам. У прстену $R = F[t, \sigma]$, полином $t^2 - 2$ је иредуцибилан, јер једначина

$$2 = (x + yu)(x + yu^2) = x^2 - xy + y^2$$

нема рационалних решења. Отуда је $K = R/(t^2 - 2)$ једно квадратно раширење тела F. ▽

Последица 2. *Ако је L/K квадратно раширење задато са (1), (2), онда се ендоморфизам α тела K може продужити до ендоморфизма $\overline{\alpha}$ тела L релацијом*

$$u^{\overline{\alpha}} = -\lambda - u,$$

и тада је δ унутрашња $\overline{\alpha}$-деривација индукована са u. Ендоморфизам $\overline{\alpha}$ је и аутоморфизам тела L акко је α аутоморфизам тела K.

Доказ: Потребно је показати да $\overline{\alpha}$ задовољава релације (1), (2) на L:

$$\overline{\alpha}(au) = \overline{\alpha}(ua^\alpha + a^\delta), \text{ тј. } a^\alpha(-\lambda - u) = (-\lambda - u)a^{\alpha^2} + a^{\delta\alpha},$$

$$(-\lambda - u)^2 + (-\lambda - u)\lambda^\alpha + \mu^\alpha = 0.$$

Прва једнакост следи из (1) и (4), док је друга последица (2) и (6). Сада (1) значи да је δ унутрашња деривација. Коначно ако је α аутоморфизам и β његов инверз, онда је $\overline{\beta}$, дефинисано са $u^{\overline{\beta}} = -\lambda^\beta - u$, инверз $\overline{\alpha}$.

Обратно, ако је $\overline{\alpha}$ аутоморфизам тела L са инверзом $\overline{\beta}$, онда за свако $a \in K$, $a^{\overline{\beta}} \in L$, рецимо

$$a^{\overline{\beta}} = ua_1 + a_2, \qquad \text{где } a_1, a_2 \in K.$$

Отуда је

$$a = -(\lambda + u)a_1^{\alpha} + a_2^{\alpha}.$$

Изједначавањем коефицијента уз u, добијамо $a_1^{\alpha} = 0$, и отуда $a_1 = 0$ и $a = a_2^{\alpha}$, што показује да је α аутоморфизам тела K. □

У комутативном случају квадратна раширења могуће је упростити допунама до потпуног квадрата и то у пољима карактеристике различите од 2. Слична редукција могућа је и у некомутативном случају.

Тврђење 3. *Нека је L/K квадратно раширење задато са* (1), (2). *Ако једначина*

$$x + x^{\alpha} = \lambda \tag{11}$$

има решења у K, онда је L/K задато елементом v који задовољава једначину

$$v^2 + v = 0. \tag{12}$$

Претходно важи ако је $\lambda^{\alpha} = \lambda$ и char $K \neq 2$.

Доказ: Ако је $x = c$ решење једначине (11) у K, заменом u са $u + c$, имамо $(u+c)^2 = u^2 + uc + cu + c^2 = -u\lambda - \mu + uc + uc^{\alpha} + c^{\delta} + c^2$ тј.

$$(u + c)^2 = c^2 + c^{\delta} - \mu.$$

Тиме важи (12) за $v = u + c$ и $\nu = \mu - c^2 - c^{\delta}$. □

Даље ћемо одредити под којим условима је квадратно раширење L/K Галуаово. Ако је L/K Галуаово раширење генерисано елементом u, онда постоји аутоморфизам тела L над K различит од идентичког. Претпоставимо да у односу на овај аутоморфизам

$$u \mapsto uc + d, \text{ где } c, d \in K, c \neq 0. \tag{13}$$

Користећи (1), за свако $a \in K$ је

$$a(uc + d) = (uc + d)a^{\alpha} + a^{\delta}.$$

Како је још $a(uc + d) = u^{\alpha}ac + a^{\delta}c + ad$, изједначавањем коефицијената уз u и 1 добијамо:

$$ca^{\alpha} = a^{\alpha}c, \tag{14}$$

$$a^{\delta}(c - 1) = da^{\alpha} - ad. \tag{15}$$

За $c \neq 1$, заменом $e = d(c-1)^{-1}$, (15) је могуће редуковати до

$$a^{\delta} = ea^{\alpha} - ae;$$

одакле је δ унутрашња деривација. За $c = 1$, (15) гласи

$$da^{\alpha} = ad. \tag{16}$$

Како по претпоставци аутоморфизам задат у (13) није идентички, то је $d \neq 0$, па је по (16) α унутрашњи аутоморфизам. Значи у квадратним Галуаовим проширењима је или α или δ унутрашње; па одговарајућим избором генератора можемо претпоставити да је или $\alpha = 1$ или $\delta = 0$. Прецизни услови формулисани су у наредној теореми.

Теорема 4. *Нека је K тело са ендоморфизмом α, α-дериватцијом δ, центром C, и L/K квадратно проширење.*

а) Ако је char $K \neq 2$, *онда је L/K Галуаово акко је δ унутрашња;*
б) ако је char $K = 2$, *онда је L/K Галуаово акко је:*

1) α унутрашњи, а δ није, нпр. $\alpha = 1$, и или је $\lambda \neq 0$ у (2) или постоји $c \in C \setminus \{0\}$ такав да је $c^\delta = c^2$, или
2) δ унутрашња, а α није, нпр. $\delta = 0$, и или је $\lambda \neq 0$ или постоји $c \in C, c \neq 1$ такав да је $cc^\alpha = 1$, или
3) и α и δ су унутрашњи нпр. $\alpha = 1, \delta = 0$ и $\lambda \neq 0$.

Доказ: а) Ако је L/K Галуаово и char $K \neq 2$, онда је као што смо већ видели или α или δ унутрашње. Уколико би α био унутрашњи, можемо узети да је $\alpha = 1$; одакле је на основу (4) 2δ унутрашња деривација индукована са λ, па је и δ унутрашња у овом случају. За $\delta = 0$ из (6), (7) следи $\lambda^\alpha = \lambda, \mu^\alpha = \mu$ и (5), (4) редукују се на

$$\mu a^{\alpha^2} = a\mu, \quad \lambda a^{\alpha^2} = a^\alpha \lambda. \tag{17}$$

Ако за генератор проширења L сада узмемо $v = 2u + \lambda$, онда је

$$v^2 = 4u^2 + 4u\lambda + \lambda^2 = \lambda^2 - 4\mu,$$

па $v \mapsto -v$ дефинише аутоморфизам L/K реда 2.

б) Претпоставимо да L/K Галуаово и да је char $K = 2$. Опет је или α или δ унутрашње тако да можемо претпоставити да је или $\alpha = 1$ или $\delta = 0$. За $\delta = 0$ из (17) следи да је α у сваком случају аутоморфизам. Сада је по (14), $c \in C$. Ако још претпоставимо да је $\lambda = 0$, онда је $u^2 + \mu = 0$ и отуда

$$\begin{aligned} 0 = (uc + d)^2 + \mu &= ucuc + ucd + duc + d^2 + \mu \\ &= u^2 c^\alpha c + uc^\delta c + ucd + ud^\alpha c + d^\delta c + d^2 + \mu \\ &= u(c^\delta c + cd + d^\alpha c) + \mu(1 + c^\alpha c) + d^\delta c + d^2. \end{aligned}$$

Изједначавањем коефицијената и користећи чињеницу да је $c \in C \setminus \{0\}$, налазимо

$$c^\delta + d + d^\alpha = 0, \tag{18}$$

$$\mu(1 + cc^\alpha) + d^\delta c + d^2 = 0. \tag{19}$$

Даље, посебно разматрамо случајеве $\alpha = 1$ и $\delta = 0$.
1) $\alpha = 1$ и δ је спољашња. По (15) је $c = 1$ тако да (18) важи, док је (19) облика

$$d^\delta = d^2. \tag{20}$$

Тако да имамо елемент $d \neq 0$ који задовољава ову једначину и који по (16) припада $C \setminus \{0\}$. Обратно, ако је $\lambda = 0$ и постоји $d \in C \setminus \{0\}$ за који важи (20), пресликавање $u \mapsto u + d$ је аутоморфизам реда 2 тела L над K, јер у том случају једнакости (14),(15),(18),(19) важе. С друге стране, ако је $\lambda \neq 0$, онда је $u \mapsto u + \lambda$ тражени аутоморфизам, јер је на основу (6) $\lambda^\delta = 0$, имајући у виду да је $\alpha = 1$.

2) $\delta = 0$ и α је спољашњи. По (15) је $d = 0$, и тиме $c \neq 1$. Опет (18) важи, док је (19) облика

$$cc^\alpha = 1. \tag{21}$$

Отуда ова једначина мора имати решење у C различито од 1. Обратно, ако (21) важи за неки елемент $c \neq 1$ у C , онда $u \mapsto uc$ дефинише аутоморфизам L/K реда 2, док за $\lambda \neq 0$ можемо опет узети $u \mapsto u + \lambda$.

3) $\alpha = 1$ и $\delta = 0$. Сада и c и d припадају C, (18) важи, а (19) је облика

$$\mu(1 + c)^2 + d^2 = 0.$$

Како је или $c \neq 1$ или $d \neq 0$, μ мора бити квадрат неког елемента из C, што противречи чињеници да $u \notin K$, па у овом случају λ мора бити различито од 0. Сада за $u \mapsto u + \lambda$ добијамо аутоморфизам L/K реда 2. □

Последица 5. *Свако квадратно раширење тела K које је коначне димензије над својим центром и карактеристике различите од 2 је Галуаово.*

Доказ: У овом случају α је унутрашњи аутоморфизам, а δ је унутрашња деривација (из тачке а) претходног доказа), па је раширење Галуаово. □

Пример 2. Нека је k тело карактеристике 0, $F = k(x)$ са аутоморфизмом $\sigma : f(x) \mapsto f(2x)$, $L = F(t; \sigma)$ и K подтело тела L генерисано са t^2 над F. Тело L је квадратно спољашње Галуаово раширење тела K.

Како $t \notin K$, то је $[1, t]$ једна база тела L над K. За произвољан елемент $p = a_0 + t^2 a_1 + \cdots + t^{2n} a_n$, $a_i \in F$ тела K важи:

$$p \cdot t = t \cdot (a_0^\sigma + t^2 a_1^\sigma + \cdots + t^{2n} a_n^\sigma),$$

па је асоцирани ендоморфизам тела K облика

$$\alpha : a_0 + t^2 a_1 + \cdots + t^{2n} a_n \mapsto a_0^\sigma + t^2 a_1^\sigma + \cdots + t^{2n} a_n^\sigma,$$

док је деривација 0. При том t поништава иредуцибилан, инваријантан полином $f = y^2 - t^2$ прстена $R = K[y; \alpha]$, па је $L = R/fR$. Сада на основу тачке а) теореме 3.4.4. следи да је L спољашње Галуаово раширење тела K. ▽

Пример 3. Нека је K тело карактеристике 2, $F = k(x)$ са деривацијом $' : f(x) \mapsto df/dx$, $L = F(t; 1, ')$ и K подтело тела L генерисано са $t^2 + t$ над F. Тело L је спољашње Галуаово раширење тела F.

Ананлогно као у претходном примеру $t \notin K$, па је $[1, t]$ једна база L/K. Сада за произвољан елемент $p = a_0 + (t^2 + t)a_1 + \cdots + (t^2 + t)^n a_n$, $a_i \in F$ тела K из једнакости

$$p \cdot t = t \cdot p + (a_0' + (t^2 + t)a_1' + \ldots (t^2 + t)^n a_n'),$$

следи да је асоцирани ендоморфизам $\alpha = 1$, а деривација δ задата са:

$$\delta : a_0 + (t^2+t)a_1 + \cdots + (t^2+t)^n a_n \mapsto a_0' + (t^2+t)a_1' + \cdots + (t^2+t)^n a_n'.$$

Уз то t поништава иредуцибилан, инваријантан полином $f = y^2 + y - (t^2+t)$ прстена $R = K[y; 1, \delta]$, па је $L = R/fR$. На основу тачке б1.) теореме 3.4.4. следи да је L спољашње Галуаово раширење тела K. ▽

3.5 Спољашња циклична Галуаова раширења

Применом резултата ове главе описаћемо спољашња Галуаова раширења са цикличном Галуаовом групом -*спољашња циклична раширења.*

Нека је K тело са ендоморфизмом α и α-деривацијом δ. Са $a', a^{(n)}$ означаваћемо редом a^δ, a^{δ^n}. Скуп

$$C = \{a \in K \mid a' = 0\} \tag{1}$$

је једно подтело тела K, које ћемо звати телом δ-константи. Посматраћемо "диференцијалну једначину"

$$p(z) = z^{(n)}a_0 + z^{(n-1)}a_1 + \cdots + za_n, \quad \text{где} \quad a_i \in K, a_0 \neq 0, \tag{2}$$

и показаћемо да је скуп елемената тела K који задовољавају једначину (2) један коначно-димензиони C-потпростор у K.

Теорема 1. *У телу K са ендоморфизмом α и α-деривацијом δ и подтелом C одређеним са* (1)*, скуп решења једначине* (2) *је леви C-простор димензије највише n.*

Доказ: Ако је $z \in K$ решење (2), онда је то и сваки елемент облика cz за $c \in C$, јер је $p(cz) = cp(z)$ за $c \in C$, чиме је први део тврђења доказан. Преостали део тврђења доказујемо индукцијом по n. Случај $n = 0$ је тривијалан. Претпоставимо да је $n > 0$ и да је још $a_n = 0$. Онда је $p = q(\delta)$ за неко q које је степена $n-1$ по δ, па је по индукцијској претпоставци $U = \ker q$ димензије $\leqslant n-1$. Нека су $u_1, \ldots, u_r$ лево C-линеарно независна решења једначине (2), при чему без умањења општости можемо претпоставити да је $u_1 = 1$ с обзиром на то да је $a_n = 0$. Сада су $u_2', \ldots, u_r'$ решења једначине $q(z) = 0$ и то лево C-линеарно независна; јер из $\sum_2^r c_i u_i' = 0$ следи $v = \sum c_i u_i \in C$. Из независности $u_1 = 1, u_2, \ldots, u_r$ следи $v = c_2 = \cdots = c_r = 0$. Стога је $r - 1 \leqslant n - 1$, тиме и $r \leqslant n$.

У општем случају ако је $a_n \neq 0$, са u означимо једно решење (2). Ако је једино решење 0, доказ је готов. Зато претпоставимо да је $u \neq 0$. Простор решења U_0 једначине $p(zu) = 0$ је димензије $\leqslant n$, јер је коефицијент уз z, $p(u) = 0$. Сада је $\ker p = \{zu \mid z \in U_0\} = U_0 u$ и исте је димензије као и U_0. □

Даље ћемо се ограничити на спољашња циклична раширења. Нека је σ генератор Галуаове групе једног таквог раширења. За $\delta = \sigma - 1$, δ је σ-деривација, јер је

$$(ab)^\delta = (ab)^\sigma - ab = a^\sigma b^\sigma - ab = (a^\sigma - a)b^\sigma + a(b^\sigma - b) = a^\delta b^\sigma + ab^\delta.$$

Приметимо да је тело δ-константи управо фиксно тело σ. По претпоставци је $\sigma^n = 1$, па је

$$h(\delta) = \sum_1^n \binom{n}{\nu} \delta^\nu = (\delta+1)^n - 1 = 0. \tag{3}$$

Најпре ћемо конструисати базу у односу не коју ће σ имати дијагоналну матрицу.

Тврђење 2. *Нека је L/K спољашње циклично раширење степена n и нека тело K садржи примитивни n-ти корен 1, нпр. ω. За сваки генератор σ Галуаове групе, L има једну базу $a_1 \ldots, a_n$ за коју је*

$$a_\nu^\sigma = \omega^\nu a_\nu, \quad \nu = 1, \ldots, n. \tag{4}$$

Доказ: Цело тело L анулира се са $h(\delta)$ које је задато са (3). Даље је $h(\delta) = \sigma^n - 1 = h_1(\delta)(\sigma - \omega)$, где је $h_1(\delta)$ степена $n-1$ по δ. По теореми 3.5.1. $\ker h_1(\delta)$ је димензије $\leq n-1$, па постоји $a \in L$ за који је $a_1 = h_1(\delta)(a) \neq 0$. Како је $h(\delta)(a) = 0$, то је $a_1^\sigma = \omega a_1$. Слично, постоји $a_\nu \neq 0$, за које је $a_\nu^\sigma = \omega^\nu a_\nu$. Треба још показати да је $[a_1, \ldots, a_n]$ десна K-база L. Претпоставимо да је $\sum a_\nu \alpha_\nu = 0$, $\alpha_\nu \in K$. Онда је $\sum \omega^{\nu^i} a_\nu \alpha_\nu = \sum a_\nu^{\sigma^i} \alpha_\nu = 0$, и како су $1, \omega, \ldots, \omega^{n-1}$ различити, следи $\alpha_\nu = 0$. Значи, $[a_1, \ldots, a_n]$ су линеарно независни и тиме чине десну базу L над K. □

Теорема 3. *За тело K са централним примитивним n-тим кореном ω из 1, постоји спољашње циклично раширење L/K степена n које садржи ω у свом центру акко постоји аутоморфизам α тела K и $a \in K$ за које је*

1) $\alpha^n = I(a), a^\alpha = a, \omega^\alpha = \omega$ *и ниједан нижи степен α није унутрашњи,* 2) $t^n a - 1$ *је иредуцибилан полином у $R = K[t; \alpha]$.*

У случају када су претходни услови задовољени $t^n a - 1$ је инваријантан у R и $L = R/(t^n a - 1)R$, а генераторни аутомофизам групе $\mathrm{Gal}(L/K)$ *је:*

$$\sigma : \sum t^\nu c_\nu \mapsto \sum (\omega t)^\nu c_\nu.$$

Доказ: Уколико важе 1), 2) $t^n a - 1$ је централан и иредуцибилан, па имамо једно спољашње циклично раширење. Обратно, за задато циклично раширење L/K на основу тврђења 3.5.2. постоји елемент $u \in L$ такав да је $u^\sigma = \omega u \neq 0$. Тада за сваки $c \in K$ важи

$$(u^{-1} c u)^\sigma = u^{-1} \omega^{-1} c \omega u = u^{-1} c u,$$

одакле је $u^{-1} c u \in K$, и тиме је $\alpha : c \mapsto u^{-1} c u$ аутоморфизам тела K и $\omega^\alpha = \omega$, тако да је са $t \mapsto u$ задат хомоморфизам $K[t; \alpha] \to L$. Језгро овог хомоморфизма генерисано је полиномом облика $t^n a - 1$, при чему a задовољава услове 1), 2). □

У цикличном раширењу L/K дефинишемо *норму* елемента $c \in L$ са

$$N(c) = c c^\sigma \ldots c^{\sigma^{n-1}}. \tag{5}$$

Последица 4. *У цикличном проширењу L/K степена n са генераторним аутоморфизмом σ, једначина*

$$cx^{\sigma} = x \tag{6}$$

има решење различито од нуле акко је

$$N(c) = 1. \tag{7}$$

Доказ: Ако једначина (6) има решење $a \neq 0$, онда је $c = a(a^{\sigma})^{-1}$, па је услов (7) задовољен. Обратно, ако важи (7), онда је $(\lambda_c \circ \sigma)^n = 1$, где λ_c означава множење слева елементом c. Тиме је

$$[(\lambda_c \circ \sigma)^n - 1](x) = 0.$$

Претходно је облика $[(\lambda_c \circ \sigma) - 1] \circ p(\sigma)(x) = 0$ за неки полином $p(\sigma)$ степена $n-1$. Сада $p(\sigma)(x) = 0$ можемо видети и као диференцијалну једначину (за $\delta = \sigma - 1$) реда $n-1$, па је њен простор решења димензије $\leqslant n-1$, тако да постоји $a \in L$ за који је $p(\sigma)(a) = b \neq 0$, чиме је $(\lambda_c \circ \sigma - 1)(b) = 0$, тј. $cb^{\sigma} = b$, тако да (6) важи за $x = b$. □

Аналогно једначина $x^{\sigma}c = x$ има решење различито од нуле акко је $c^{\sigma^{n-1}} \dots c^{\sigma}c = 1$.

Следеће тврђење даће нам особине факторизација полинома $t^n - a$ за $a \in K$.

Тврђење 5. *У телу K са аутоморфизмом σ реда n и примитивним n-тим кореном из 1 који је у центру тела K за сваки $a \in K$ полином $t^n - a$ је или иредуцибилан у $K[t;\alpha]$ или је производ фактора истог степена. Специјално, ако је n прост, $t^n - a$ је или производ линеарних фактора или иредуцибилан у зависности од тога да ли једначина*

$$N(x) = xx^{\sigma} \dots x^{\sigma^{n-1}} = a$$

има решења или не.

Доказ: Ако је $p(t)$ иредуцибилан леви фактор $t^n - a$, онда је то и $p(\omega^{\nu}t)$, за $\nu = 1, \dots, n-1$, тако да је

$$t^n - a = p_1 \dots p_r q,$$

где је $p_1(t) = p(t)$ и сваки p_i је сличан неком $p(\omega^{\nu_i}t)$ за неко ν_i. Ако је изабрано највеће могуће r, онда је сваки $p(\omega^{\nu}t)$ фактор $p_1 \dots p_r$ и то је заправо њихов најмањи заједнички садржалац, који се не мења заменом $t \mapsto \omega t$. То значи да је овај полином по t^n позитивног степена и фактор $t^n - a$, па је једнак $t^n - a$, одакле је $q = 1$. Тиме је доказан први део тврђења.

Ако је p степена d, онда $d \mid n$, па ако је n прост, d је 1 или n. Последњи део тврђења последица је идентитета:
$t^n - a = (t-b)(t^{n-1} + t^{n-2}b^{\sigma^{n-1}} + \dots + b^{\sigma}b^{\sigma^2} \dots b^{\sigma^{n-1}}) + b^{\sigma}b^{\sigma^2} \dots b^{\sigma^{n-1}} - a.$ □

Посматраћемо, даље случај када је n степен карактеристике тела, тј. $n = p^e, p = \operatorname{char} K$. У овом случају једнакост (3) своди се на $\delta^n = 0$.

Тврђење 6. *Нека је L/K спољашње циклично раширење степена $n = p^e$, где је $p = \Gamma K$, са аутоморфизмом $\sigma = \delta + 1$. Скуп $L_\nu = \ker \delta^\nu = \{c \in L \mid c^{(\nu)} = 0\}$ је десни K-простор димензије ν и*

$$K \subseteq L_1 \subseteq L_2 \subseteq \ldots L_n = L,\ L_\nu = L'_{\nu+1}\ (\nu = 1, \ldots, n-1).$$

Доказ: По теореми 3.7.1., $[L_\nu : K]_R \leqslant \nu$, док за $\nu = n$ важи једнакост. Доказ ћемо извести индукцијом по $n - \nu$. Претпоставимо да је $a_0 = 1, a_1, \ldots, a_\nu$ десна K-база простора $L_{\nu+1}$. Тврдимо да је $a'_0 = 1, a'_1, \ldots, a'_\nu$ десна K-база простора L_ν. Ако је $\sum a'_i c_i = 0$, онда је $\sum a_i c_i = c \in K$. Како су $a_0, \ldots, a_\nu$ линеарно независни, то је $c_1 = \cdots = c_\nu = 0$, па су и $a'_1, \ldots, a'_\nu$ линеарно независни; такође припадају L_ν, што показује да је $L_\nu = L'_{\nu+1}$ и $[L_\nu : K]_R = \nu$. □

Како је $L' = L_{n-1}$ имамо следећи критеријум:

Последица 7. *Под претпоставкама тврђења* 3.7.6., *једначина $x' = a$ $(a \in L)$ има решења у L акко је $a^{(n-1)} = 0$.* □

Ако је ν степен p, нпр. $\nu = p^i$, L_ν можемо описати и као фиксни скуп аутоморфизма σ^ν, што је последица једнакости $\delta^\nu = (\sigma - 1)^\nu = \sigma^\nu - 1$.

У спољашњем цикличном проширењу дефинишемо и *траг* елемента $a \in L$ са

$$\operatorname{tr} a = \sum_0^{n-1} a^{\sigma^\nu}.$$

Како је

$$\delta^{n-1} = (\sigma - 1)^{n-1} = \frac{(\sigma - 1)^n}{\sigma - 1} = \frac{\sigma^n - 1}{\sigma - 1} = \sum_0^{n-1} \sigma^\nu,$$

следи

$$\operatorname{tr} a = a^{(n-1)} \quad \text{за свако } a \in L. \tag{8}$$

Ова формула омогућава нам да докажемо теорему о нормалној бази. За базу Галуаовог проширења кажемо да је *нормална* ако се састоји од конјугата неког елемента. Такав елемент зваћемо *примитивним*.

Теорема 8. *Свако спољашње циклично раширење L/K степена $n = p^e$, где је $p = \operatorname{char} K$, има нормалну базу, и $a \in L$ је примитиван акко је $\operatorname{tr} a \neq 0$.*

Доказ: На основу (8), $\operatorname{tr} a \neq 0$ акко $a \notin L_{n-1}$, тако да за свако $a \notin L_{n-1}$ имамо $a^{(n-\nu)} \in L_\nu \setminus L_{\nu-1}$ и $[a, a', \ldots, a^{(n-1)}]$ је једна база $L_n = L$. □

Одредићемо још и проширења степена p. Користићемо Џејкобсон-Шазенхаусову формулу за тела карактеристике p:

$$(x+y)^p - (x+y) = x^p - x + y^p - y + \Lambda(x, y), \tag{9}$$

где је Λ сума комутатора по x и y. Израз

$$V(x) = (t+x)^p - (t+x) - t^p + t = (t+x)^p - t^p - x. \tag{10}$$

у прстену $K[t; 1, \delta]$ је полином по $x, x', \ldots, x^{(p-1)}$, јер је $[x, t] = xt - tx = x'$. Доказаћемо прво тврђење аналогно 3.7.5.:

Тврђење 9. *У телу K карактеристике p са дериваџијом δ за коју је $\delta^p = 0$ за свако $a \in K$ полином $t^p - t - a \in K[t; 1, \delta]$ је или производ линеарних фактора који комутирају или иредуџибилан у зависности да ли једначина*

$$V(x) + a = 0,$$

има решења у K или не.

Доказ: Ако је h моничан иредуџибилан фактор полинома $t^p - t - a$, степена d, онда су полиноми $h(t+\nu)$ $(\nu = 0, 1, \ldots, p-1)$ слични факторима полинома $t^p - t - a$. Њихов најмањи заједнички садржалац је инваријантан при пресликавању $t \mapsto t+1$, па је степена $\geqslant p$, али као фактор $t^p - t - a$ једнак је $t^p - t - a$. Сви $h(t+\nu)$ су иредуџибилни и истог степена d, тако да $d \mid p$ и тиме $d = 1$ или $d = p$. Ако је $V(b) + a = 0$, онда је $(t+b)^p - (t+b) - t^p + t = V(b) = -a$, и отуда

$$t^p - t - a = (t+b)^p - (t+b) = (t+b)((t+b)^{p-1} - 1),$$

тако да је $t^p - t - a$ производ линеарних фактора $t + b + \nu$ $(\nu = 0, 1 \ldots, p-1)$, који међусобно комутирају. Обратно, ако је $t+b$ линеаран фактор $t^p - t - a$ онда је

$$(t+b)^p - (t+b) - V(b) - a = t^p - t - a = (t+b)h(t),$$

и тиме $V(b) + a$ има фактор $t + b$, али како је $V(b)$ степена 0 по t, то је $V(b) + a = 0$. □

Сада ћемо доказати теорему аналогну теореми 3.7.3. за спољашња циклична раширења степена p:

Теорема 10. *Тело K карактеристике p има спољашње циклично раширење L степена p акко постоји спољашња дериваџија δ на K за коју је*

1) *$\delta^p - \delta$ унутрашња, индукована са $a \in K$, $a^\delta = 0$, и*
2) *$V(x) + a$ нема решења у K.*

Уколико претходни услови важе $t^p - t - a$ је инваријантан и иредуџибилан полином у $R = K[t; 1, \delta]$; $L = R/(t^p - t - a)R$, са генераторним аутоморфизмом

$$\sigma : \sum t^\nu c_\nu \mapsto \sum (t+1)^\nu c_\nu.$$

Доказ: Уколико важе 1) и 2) $t^p - t - a$ је централан и иредуџибилан, и тиме имамо једно спољашње циклично раширење.

Обратно, нека је L/K спољашње циклично раширење степена p са генераторним аутоморфизмом σ. На основу 3.7.6. у L постоји елемент y за који је $y^\sigma = y + 1$, одакле пресликавање $c \mapsto c^\delta = cy - yc$ индукује дериваџију на K, за коју је пресликавање $t \mapsto y$, $K[t; 1, \delta] \to L$ хомоморфизам. При том је $y^p - y = a \in K$, па је $\delta^p - \delta$ унутрашња, индукована са a, и $a^\delta = 0$, док $V(x) + a = 0$ нема решења у K, услед иредуџибилности полинома $y^p - y - a$ над K. □

4

О ЈЕДНОЈ ПРИМЕНИ КОСИХ ПОЛИНОМА

4.1 Нуле косих полинома

Нека је K тело са ендоморфизмом α и α-дериватцијом δ. Као што смо видели у прстену косих полинома $R = K[t;\alpha,\delta]$ важи Еуклидов алгоритам дељења тако да сваки $f(t) \in R$ за $g(t) \in R \setminus \{0\}$ можемо на јединствен начин представити у облику $f(t) = g(t)q(t) + r(t)$, где је $\deg r(t) < \deg g(t)$. С обзиром на то да у комутативном случају вредност полинома $f(t)$ у тачки a можемо видети као остатак при дељењу полинома $f(t)$ полиномом $t-a$ и да у нашем случају важи алгоритам дељења, дефинисаћемо вредност косог полинома $f(t)$ у тачки $a \in K$ на аналоган начин. Ако за $a \in K$ дефинишемо $N_0(a) = 1$ и даље индуктивно $N_{n+1}(a) = aN_n(a)^\alpha + N_n(a)^\delta$, вредност полинома $f(t) = a_0 + ta_1 + \cdots + t^n a_n$ у a можемо израчунати и помоћу формуле

$$f(a) = \sum N_i(a)a_i.$$

За елемент $a \in K$ рећи ћемо да је *нула* полинома $f(t) \in R$ ако је $f(a) = 0$, тј. ако је остатак при дељењу $f(t)$ са $t - a$ нула. Елемент облика

$$b^{-1}ab^\alpha + b^{-1}b^\delta$$

зваћемо (α,δ)-конјугатом елемента a. У односу на ове дефиниције важе аналогни ставови ставовима из 3.2.

Теорема 1. *Нека је $f(t) = g(t)h(t) \in R$ и $a \in K$. Ако је $g(a) = 0$ онда је и $f(a) = 0$. Ако је a нула полинома $f(t)$, а није нула полинома $g(t)$ онда је један (α,δ)-конјугат нула полинома $h(t)$.*

Доказ: За

$$f(t) = (t-a)q(t) + f(a),$$
$$g(t) = (t-a)q_1(t) + g(a),$$
$$h(t) = (t-a)q_2(t) + h(a)$$

једнакост $f(t) = g(t)h(t)$ је облика

$$f(t) = (t-a)(q_1(t)(t-a)q_2(t) + q_1h(a)) + g(a)(t-a)q_2(t) + g(a)h(a),$$

одакле очигледно из $g(a) = 0$ следи $f(a) = 0$. Претпоставимо сада да је $a \in K$ нула полинома $f(t)$, а да је при том $b = g(a) \neq 0$. У овом случају је

$$f(t) = (t-a)q(t) = ((t-a)q_1 + b)h(t)$$

одакле је

$$h(t) = b^{-1}((t-a)(q(t) - q_1(t)h(t)) = (t(b^{-1})^{\alpha} + (b^{-1})^{\delta} - b^{-1}a)(q(t) - q_1(t)h(t)),$$

што за последицу има

$$h(b^{-1}ab^{\alpha} - (b^{-1})^{\delta}b^{\alpha}) = 0.$$

Пошто је δ α-деривација, из $0 = 1^{\delta} = (b^{-1}b)^{\delta} = (b^{-1})^{\delta}b^{\alpha} + b^{-1}b^{\delta}$ добијамо $(b^{-1})^{\delta}b^{\alpha} = -b^{-1}b^{\delta}$. Значи, ако је a нула полинома $f(t)$, а није нула полинома $g(t)$ онда је њен (α, δ)-конјугат нула полинома $h(t)$. □

Користећи претходну теорему добијамо:

Последица 2. *За полином $f(t) \in K[t; \alpha, \delta]$, $f(a) = 0$ акко је $f(t) = (t-a)g(t)$ за неко $g(t) \in K[t; \alpha, \delta]$.* □

Последица 3. *Нуле полинома $f(t) \in K[t; \alpha, \delta]$ степена n елементи су највише n (α, δ)-класа конјугације тела K. Ако је $f(t)$ облика $(t-a_1)\dots(t-a_n)$ где $a_1, \dots, a_n \in K$, онда је свака нула полинома f (α, δ)-конјугована са неким a_i.* □

Пример 1. Илустоваћемо претходна тврђења на примеру прстена $R = k[t; 1, \prime]$, где је $k = F(x)$ поље рационалних функција над пољем F. Нека је

$$a = t^2 - t\frac{1}{x}$$

фиксиран елемент овог прстена. Он се очигледно може факторисати као:

$$t^2 - t\frac{1}{x} = t(t - \frac{1}{x}).$$

Ако пробамо да факторишемо елемент a на неки други начин,

$$t^2 - t\frac{1}{x} = (t - A(x))(t - B(x)) = t^2 - t(A(x) + B(x)) + A(x)B(x) - A'(x)$$

долазимо до једнакости $A(x) + B(x) = 1/x, \quad A(x)B(x) - A'(x) = 0$. Одавде добијамо са $A(x)$ мора бити решење Рикатијеве једначине

$$A' + A^2 = A \cdot (1/x).$$

Једно партикуларно решење ове једначине је $A(x) = 2/x$, па за $B(x) = 1/x - A(x)$, односно $B(x) = -1/x$ добијамо још једну нетривијалну факторизацију елемента a:

$$t^2 - t\frac{1}{x} = (t - \frac{2}{x})(t + \frac{1}{x}).$$

Опште решење диференцијалне једначине $A' + A^2 = A \cdot (1/x)$ дато је формулом $A(x) = 2/x + 2/(2ct^3 - t)$, па нпр. за $c = 1/2$ добијамо рационалну функцију $A(x) = 2x/(x^2 - 1)$ и одговарајућу функцију

$$B(x) = -(x^2 + 1)/x(x^2 - 1).$$

Факторизација елемента a сада има облик:

$$t^2 - t\frac{1}{x} = (t - \frac{2x}{x^2 - 1})(t + \frac{x^2 + 1}{x(x^2 - 1)}).$$

Ова разлагања су изоморфна и одговарајуће нуле $A(x)$ елементи су исте класе $(1,\prime)$-конјугације. ∇

У наредном делу посматраћемо само прстене косих полинома у којима је $\delta = 0$. С тим у вези елемент облика $b^{-1}ab^{\alpha}$ звaћемо *α-конјугатом* елемента a.

За скуп $\Delta \subset K$ кажемо да је *α-алгебарски* ако постоји полином $f \in K[t;\alpha]$ различит од нуле који се анулира на скупу Δ. Скуп $I(\Delta)$, полинома који се анулирају на скупу Δ је десни идеал прстена $K[t;\alpha]$. Ако је f моничан полином најмањег степена у $I(\Delta)$, онда је $I(\Delta) = f \cdot K[t;\alpha]$. Полином f са овим својством јединствено је одређен. Означаваћемо га са f_Δ и звати *минималним* полиномом скупа Δ. Степен полинома f_Δ звaћемо *рангом* скупа Δ.

Лема 4. *Ако је Δ α-алгебарски скуп ранга n, онда је $f_\Delta(t) = (t-a_1)\dots(t-a_n)$, где је сваки од a_i α-конјугован са неким елементом из Δ.*

Доказ: За свако $a \in \Delta$, $t - a$ је леви фактор полинома $f_\Delta(t)$. Нека је m највећи природан број за који $f_\Delta(t)$ има леви фактор облика $h(t) = (t-a_1)\dots(t-a_m)$, где је сваки a_i α-конјугован неком елементу из Δ. Треба још показати да је $m = n$. Уколико је $m < n$, постоји $d \in \Delta$ за који је $h(d) \neq 0$ (јер се полином h не анулира на Δ). Како је $f_\Delta(t) = h(t)g(t)$ на основу теореме 4.1.2. α-конјугат d' од d је нула полинома $g(t)$, па је у том случају $t - d'$ леви фактор $g(t)$, а $(t-a_1)\dots(t-a_m)(t-d')$ леви фактор полинома f_Δ. Контрадикција! □

Тврђење 5. *Коначан скуп $\Delta \subset K$ је увек α-алгебарски ранга $\leqslant |\Delta|$.*

Доказ: Довољно је показати да постоји полином степена $r \leqslant |\Delta|$ који се анулира на Δ. То ћемо показати индукцијом по r. За $r = 1$, тривијално важи. Нека је $r \geqslant 2$ и $f(t) = (t - a)g(t)$ за неко $a \in \Delta$. Ако се f анулира на $\Delta_0 = \Delta \setminus \{a\}$, онда се g анулира на скупу

$$\Delta' = \{(b-a)^{-1}b(b-a)^{\alpha} \mid b \in \Delta_0\}.$$

Како је $|\Delta'| \leqslant r - 1$, по индукцијској претпоставци можемо изабрати полином g степена $\leqslant r - 1$. □

Пример 2. За $\Delta = \{a, b\}$ је

$$f_{\{a,b\}}(t) = (t - a)(t - (b-a)^{-1}b(b-a)^{\alpha}).$$

∇

4.2 Уопштена Вандермондова матрица

Вандермондовом матрицом над пољем K зовемо матрицу

$$V_n(a_1,\dots,a_n)=\begin{bmatrix} 1 & 1 & \dots & 1 \\ a_1 & a_2 & \dots & a_n \\ \vdots & \vdots & & \vdots \\ a_1^{n-1} & a_2^{n-1} & \dots & a_n^{n-1} \end{bmatrix}.$$

Њена детерминанта је $\det V_n(a_1,\dots,a_n)=\prod_{i>j}(a_i-a_j)$. Отуда је Вандермондова матрица инвертибилна акко међу елементима $a_1,\dots,a_n$ нема једнаких.

Уопштење Вандермондове матрице извршићемо по два основа:

1) дозволићемо да елементи матрице припадају телу,
2) укључићемо и произвољан ендоморфизам α тела K.

Прецизније, за задате елементе $a_1,\dots,a_n$ тела K и ендоморфизам $a\mapsto a^\alpha$ тела K, дефинишемо α-Вандермондову матрицу са

$$V_n^\alpha(a_1,\dots,a_n)=\begin{bmatrix} 1 & 1 & \dots & 1 \\ N_1(a_1) & N_1(a_2) & \dots & N_1(a_n) \\ \vdots & \vdots & & \vdots \\ N_{n-1}(a_1^{n-1}) & N_{n-1}(a_2^{n-1}) & \dots & N_{n-1}(a_n^{n-1}) \end{bmatrix}$$

где је $N_i(a)=aa^\alpha\dots a^{\alpha^{i-1}}$. Специјално за $\alpha=1$ добијамо обичну Вандермондову матрицу.

Пример 1. За $K=\mathbb{C}$ и $\alpha(z)=\overline{z}$, α-Вандермондова матрица формата 3×3 је облика

$$V_3^\alpha(a,b,c)=\begin{bmatrix} 1 & 1 & 1 \\ a & b & c \\ |a|^2 & |b|^2 & |c|^2 \end{bmatrix}.$$

Њена детерминанта је

$$\det V_3^\alpha(a,b,c)=-a(|c|^2-|b|^2)+b(|c|^2-|a|^2)-c(|b|^2-|a|^2). \qquad (1)$$

Претпоставимо да су $|a|,|b|,|c|$ различити, нпр. $|a|<|b|<|c|$ (ово можемо постићи пермутацијама колона). Двоструком применом неједнакости $|x-y|\geqslant|x|-|y|$ добијамо

$$\begin{aligned} |V_3^\alpha(a,b,c)| &\geqslant |b(|c|^2-|a|^2)|-|a(|c|^2-|b|^2)|-|c(|b|^2-|a|^2)| \\ &= -|a|(|c|^2-|b|^2)+|b|(|c|^2-|a|^2)-|c|(|b|^2-|a|^2) \\ &= \det V_3(|a|,|b|,|c|) \\ &= (|c|-|b|)(|c|-|a|)(|b|-|a|)>0 \end{aligned}$$

Значи, $V_3^\alpha(a,b,c)$ је инвертибилна ако су $|a|,|b|,|c|$ различити. С друге стране, ако је $|a|=|b|\neq|c|$ из једнакости (1), имамо

$$\det V_3^\alpha(a,b,c)=(a-b)(|b|^2-|c|^2)\neq 0,$$

па је $V_3^\alpha(a,b,c)$ опет инвертибилна. За $|a|=|b|=|c|$ је $\det V_3^\alpha(a,b,c)=0$ и то је једини случај у ком $V_3^\alpha(a,b,c)$ није инвертибилна. ∇

Пример 2. Нека је $V_3(a,b,c)$ Вандермондова матрица над произвољним телом K $(\alpha = 1)$ и претпоставимо да су a,b,c различити. Множењу слева елементарном матрицом у наредној једнакости одговарају две узастопне елементарне операције на врстама матрице $V_3(a,b,c)$:

$$\begin{bmatrix} 1 & 0 & 0 \\ -a & 1 & 0 \\ 0 & -a & 1 \end{bmatrix} V_3(a,b,c) = \begin{bmatrix} 1 & 1 & 1 \\ 0 & b-a & c-a \\ 0 & (b-a)b & (c-a)c \end{bmatrix}. \tag{2}$$

У вези са једнакошћу (2) посматрамо матрицу M формата 2×2:

$$M = \begin{bmatrix} b-a & c-a \\ (b-a)b & (c-a)c \end{bmatrix}.$$

У матрици M не можемо издвојити факторе $b-a$ и $c-a$ из прве односно друге колоне с обзиром на то да су оба леви фактори, а у елементарним операцијама на колонама дозвољено је једино множење здесна. Матрицу M даље трансформишемо:

$$\begin{bmatrix} (c-a)^{-1} & 0 \\ 0 & (c-a)^{-1} \end{bmatrix} M = \begin{bmatrix} (c-a)^{-1}(b-a) & 1 \\ (c-a)^{-1}(b-a)b & c \end{bmatrix},$$

и применом још једне операције на врстама последње матрице добијамо матрицу:

$$\begin{bmatrix} (c-a)^{-1}(b-a) & 1 \\ (c-a)^{-1}(b-a)b - c(c-a)^{-1}(b-a) & 0 \end{bmatrix}.$$

Из последњег можемо закључити да је за различите $a,b,c \in K$, матрица $V_3(a,b,c)$ сингуларна акко је $(c-a)^{-1}(b-a)b = c(c-a)^{-1}(b-a)$, или еквивалентно

$$(b-a)b(b-a)^{-1} = (c-a)c(c-a)^{-1}. \tag{3}$$

Претходни рачун има непосредне везе са рачунањем *Диодонеове детерминанте*, која представља уопштење детерминанти над телима. ▽

Укратко ћемо описати, како се дефинише *Доидонеова детерминанта* (детаљније [3],[9]).

Нека је K тело и $A = [a_{ij}] \in M_n(K)$. За свако $i \neq j$ и $\lambda \in K$ са $B_{ij}(\lambda)$ означаваћемо матрицу добијену из јединичне заменом елемента $a_{ij} = 0$ елементом λ. Множењем слева (здесна) матрице A матрицом $B_{ij}(\lambda)$ добијамо матрицу која настаје из A додавањем i-тој врсти j-те која је претходно помножена слева са λ (додавањем j-тој колони i-те помножене здесна са λ). Посебно је

$$B_{ij}(\lambda)B_{ij}(\mu) = B_{ij}(\lambda+\mu), \quad B_{ij}(\lambda)^{-1} = B_{ij}(-\lambda).$$

Матрице $B_{ij}(\lambda)$, за $i \neq j$, $\lambda \in K$ генеришу једну подгрупу групе $Gl_n(K)$ коју ћемо звати *унимодуларном* подгрупом и означавати са $Sl_n(K)$.

Претпоставимо да је матрица A инвертибилна. Тада је бар један елемент њене прве колоне различит од нуле. Ако је $n > 2$ и $a_{21} = 0$, додамо одговарајућу врсту другој, чиме добијамо матрицу у којој је $a_{21} \neq 0$.

Сада множимо другу врсту са $(1-a_{11})a_{21}^{-1}$ и додамо првој. У тако добијеној матрици је $a_{11}=1$. Множењем прве врсте са a_{i1} и одузимањем од i-те $(i>1)$, добијамо матрицу у којој је $a_{11}=1, a_{i1}=0, i>1$. Преосталих $n-1$ врста матрице A су линеарно независне, па аналогним поступком на другој колони добијамо матрицу у којој је $a_{22}=1, a_{2i}=0, i>2$. Такође можемо постићи $a_{12}=0$ одузимањем друге врсте помножене са a_{12} од прве. Поступак настављамо све док не добијемо дијагоналну матрицу $D(\mu)$ са дијагоналним компонентама $a_{11}=\cdots=a_{n-1n-1}=1, a_{nn}=\mu$, при чему је $\mu\neq 0$. Из претходног важи:

Теорема 1. *Свака инвертибилна матрица $A\in M_n(K)$ је облика $B\cdot D(\mu)$ за неку матрицу $B\in Sl_n(K)$ и неко $\mu\neq 0$.* □

Означимо са K^{ab} абелизацију групе $K^\times$, тј. $K^{ab}=K^\times/[K^\times,K^\times]$. Свакој инвертибилној матрици $A\in M_n(K)$ придружићемо један елемент из K^{ab}, који ћемо звати Диодонеовом детерминантом матрице A, и то $\mu\cdot[K^\times,K^\times]$ ако је $A=B\cdot D(\mu)$. За неинвертибилне матрице A дефинишемо $\det A=0\cdot[K^\times,K^\times]$.

У примеру 4.2.2. Диодонеова детерминанта матрице $V_3(a,b,c)$ је косет елемента

$$-(c-a)^2[(c-a)^{-1}(b-a)b-c(c-a)^{-1}(b-a)]=(c-a)[(c-a)c(c-a)^{-1}(b-a)-(b-a)b].$$

Приметимо да се у случају када a,b,c комутирају Диодонеова детерминанта своди на Вандермондову детерминанту $(c-a)(b-a)(c-b)$, као и да услов (3), који је довољан за сингуларност матрице $V_3(a,b,c)$, има још два еквивалентна облика:

$(a-b)a(a-b)^{-1}=(c-b)b(c-b)^{-1}$,

$(a-c)a(a-c)^{-1}=(b-c)b(b-c)^{-1}$.

Један од потребних услова за инвертибилност матрице $V_3(a,b,c)$ је да a,b,c, нису по паровима конјуговани, тј. да a,b,c нису у истој класи конјугације тела K.

Пример 3. У телу $\mathbb{H}$ реалних кватерниона, елементи $a=i,b=j,c=k$ су конјуговани, па је матрица $V_3(i,j,k)$ сингуларна. ▽

4.3 Ранг α-Вандермондове матрице

Већ је показано да је квадратна матица формата n инвертибилна акко је њен ранг n. С тим у вези одредићемо ранг Вандермондове матрице и на тај начин добићемо критеријум њене инвертибилности. Ако је $V=V_n^\alpha(a_1,\ldots,a_n)$ α-Вандермондова матрица са $\Delta\subset K$ означићемо скуп $\{a_1,\ldots,a_n\}$.

Теорема 1. $\operatorname{rang} V=\operatorname{rang}\Delta$.

Доказ: Означимо са r,c,d редом ранг врста, ранг колона матрице V и ранг скупа Δ. Показаћемо да је $r\leqslant d\leqslant c$. Имајући у виду да је $r=c$ претходна неједнакост даће тражени резултат.

У доказу ћемо користити следеће: полином $g(t) = \sum_{i=0}^{n-1} b_i t^i \in K[t;\alpha]$ (елементи $K[t;\alpha]$ су нам сада десни полиноми, а правило комутирања задато је са $ta = a^\alpha t$) анулира се на скупу Δ акко је $(b_o,\ldots,b_{n-1})V = 0$. За неједнакост $d \leqslant c$ довољно је наћи полином $g(t) \in K[t;\alpha]$ степена $\leqslant c$ који се анулира на Δ. Матрица V има c линеарно независних колона. Без умањења општости претпоставимо да је то првих c колона. Нека је $g(t) = \sum b_i t^i$ минимални полином скупа $\{a_1,\ldots,a_c\}$. На основу тврђења 4.1.5. је $\deg g \leqslant c \leqslant n$ и $(b_o,\ldots,b_{n-1})C_i = 0$ за $1 \leqslant i \leqslant c$. Како је свака колона C_j десна линеарна комбинација колона $C_1,\ldots,C_c$, такође је $(b_o,\ldots,b_{n-1})C_j = 0$ и тиме $(b_o,\ldots,b_{n-1})V = 0$, тј. $g(\Delta) = 0$. Даље, нека је $f = f_\Delta(t)$ минимални полином скупа Δ. За неједнакост $r \leqslant d$ довољно је показати да је свака врста R_i матрице V лева линеарна комбинација првих d врста $R_1,\ldots,R_d$. Применом (левог) алгоритма дељења је

$$t^i = q(t)f(t) + e_0 + e_1 t + \cdots + e_{d-1}t^{d-1},$$

јер је $d = \operatorname{rang}\Delta$ степен полинома f. Заменом a_j у претходној једнакости добијамо

$$N_i(a_j) = e_0 + e_1 N_1(a_j) + \cdots + e_{d-1}N_{d-1}(a_j).$$

Тиме је $R_i = e_0 R_1 + e_1 R_2 + \cdots + e_{d-1}R_d$, што је и требало показати. □

Проширићемо претходни резултат на правоугаоне α-Вандермондове матрице, $V^\alpha_{m,n}(a_1,\ldots,a_n)$ формата $m \times n$ којима је $(i+1)$-ва врста

$$(N_i(a_1),\ldots,N_i(a_n)).$$

Лема 2. *За $m \geqslant n$ је* $\operatorname{rang} V^\alpha_{m,n}(a_1,\ldots,a_n) = \operatorname{rang} V^\alpha_n(a_1,\ldots,a_n)$.

Доказ: Нека су $f(t)$ и d као у доказу претходне теореме. Последњи део претходног доказа можемо применити на било коју врсту матрице $V^\alpha_{m,n}(a_1,\ldots,a_n)$. Тиме је ранг врста $V^\alpha_{m,n}(a_1,\ldots,a_n) \leqslant d$, тј. од ранга врста $V^\alpha_n(a_1,\ldots,a_n)$. Обратна неједнакост тривијално важи. □

Последица 3. *Ако је нека $n \times n$ подматрица матрице $V^\alpha_{m,n}(a_1,\ldots,a_n)$ $(m \geqslant n)$ инвертибилна, онда је и матрица $V^\alpha_n(a_1,\ldots,a_n)$ инвертибилна.* □

У комутативном случају на основу претходне последице важи следеће: ако је $\det V^\alpha_n(a_1,\ldots,a_n) = 0$, онда је детерминанта сваке $n \times n$ подматрице $V^\alpha_{m,n}(a_1,\ldots,a_n)$, $(m \geqslant n)$ такође нула. Применом претходних тврђења одредићемо формулу за ранг матрице $V^\alpha_{m,n}(a_1,\ldots,a_n)$.

Теорема 4. $\operatorname{rang} V^\alpha_{m,n}(a_1,\ldots,a_n) = \min\{m, \operatorname{rang}\Delta\}$

Доказ: Ако је $d = \operatorname{rang}\Delta$ претпоставићемо да је првих d колона у $V^\alpha_n(a_1,\ldots,a_n)$ десно линеарно независно. Тиме је и матрица $V^\alpha_{n,d}(a_1,\ldots,a_d)$ ранга d, као и $V^\alpha_{d,d}(a_1,\ldots,a_d)$ (на основу леме 4.3.2.). Тиме је првих d врста матрице $V^\alpha_{d,d}(a_1,\ldots,a_d)$ лево линеарно независно, одакле исто важи и за $V^\alpha_n(a_1,\ldots,a_n)$. Ако је $m \leqslant d$, онда је очигледно $\operatorname{rang} V^\alpha_{m,n}(a_1,\ldots,a_n) = m = \min\{m,d\}$. Зато претпоставимо да је $m > d$. Ако је $m \geqslant n$ доказ завршава лема 4.3.2., док је у супротном $\operatorname{rang} V^\alpha_{m,n}(a_1,\ldots,a_n) \leqslant \operatorname{rang} V^\alpha_n(a_1,\ldots,a_n) = d$. Како је првих d колона матрице $V^\alpha_{m,n}(a_1,\ldots,a_n)$ лево линеарно независно, то важи и обрнута неједнакост и тиме $\operatorname{rang} V^\alpha_{m,n}(a_1,\ldots,a_n) = d = \min\{m,d\}$.

Пример 1. Нека је $K = \mathbb{Q}(a)$ и $\mu_a(t) = t^3 + t^2 - 2t - 1$ минимални полином a над $\mathbb{Q}$. Тада је K Галуаово раширење поља $\mathbb{Q}$ и преостале две нуле полинома μ_a су $a^2 - 2$ и $1 - a - a^2$. Конструишемо тело $D = K + Kx + Kx^2$, где x задовољава релације $x^3 = 2$ и $xa = (a^2 - 2)x$. Ове релације и њихове последице задају множење на D, у односу на које је D једна 9-димензионална алгебра са центром $\mathbb{Q}$. За $b = xax^{-1} = a^2 - 2$ посматрамо квадратни полином

$$f(t) = (t - a)(t - b) = t^2 - (a + b)t + ab \in D[t].$$

И a и b су нуле полинома $f(t)$, с обзиром на то да комутирају. Испитаћемо да ли међу другим конјугатима dad^{-1} има нула полинома f. У том случају мора да важи $da^2d^{-1} - (a + b)dad^{-1} + ab = 0$ или еквивалентно

$$da^2 - (a + b)da + abd = 0.$$

Претходна једнакост важи за $d = 1$ и $d = x$ и пошто је линеарна по d важи ће и за $d = 1 + x$. Тиме је трећи корен полинома f

$$c = (1 + x)a(1 + x)^{-1} = ((a + 2b) + (b - a)x + (a - b)x^2)/3.$$

Полином f је такође и минимални полином скупа $\Delta = \{a, b\}$, па је тиме $\operatorname{rang} V_3(a, b, c) = 2$.

∇

Литература

[1] S. Annin, *Associeted Primes over Skew Polynomials Rings*, Comm. in Algebra **30** (2001), 2511-2528.

[2] S. Annin, *Associeted and Attached Primes over Noncommutative Rings*,

[3] E. Artin, *Geometric Algebra*, Interscience Publishers, inc., New York, 1957.

[4] P.M. Cohn, *Skew Field Constructions*, Cambrige University Press, 1977.

[5] P.M. Cohn, *Universal Algebra*, Reidel, Dordrecht, 1981.

[6] P.M. Cohn, *Free Rings and their Relations*, Academic Press Inc. London, 1985.

[7] P.M. Cohn, *Algebra, vol.3*, Wiley and Sons, Chichester, 1991.

[8] P.M.Cohn, *Skew Fields*, Cambrige University Press, 1995.

[9] J. Dieudonné, *Les déterminants sur un corps non-commutatif*, Bull. Soc. Math. France **71** (1943), 27-45,

[10] A.V. Jategaonakar, *Ore Domains and Free Algebras*, Bull. London Math. **1** (1969), 45-46.

[11] A.V. Jategaonakar, *An Operator Theory of Linear Functional Differential Equations*, J.Diff. Equations **27** (1978), 274-297.

[12] G.Kalajdzić, M. Đorić, *Geometrija*, Matematički fakultet, Beograd, 2003.

[13] T.Y. Lam, *A First Course in Noncommutatative Rings*, Springer-Verlag, 1991.

[13] T.Y. Lam, *Exercises in Classical Ring Theory*, Springer-Verlag, 1995.

[15] T.Y. Lam, *A General Theory of Vandermonde Matrices*, Expo. Math. **4** (1986), 193-215.

[16] André Leroy, T.Y. Lam, *Vandermonde and Wronskian Matrices over Division Rings*, J. Algebra **119** (1988), 308-336.

[17] André Leroy, T.Y. Lam, *Homomorphisms between Ore Extensions*, Contemporary Mathematics **124** (1992), 83-110.

[18] André Leroy, T.Y. Lam, *Principal one-sided Ideals in Ore Polynomial Rings*, Contemporary Mathematics **259** (1999), 333-352.

[19] J. Matzuk, T.Y. Lam, André Leroy, *Primeness, Semiprimeness and Prime Radical of Ore Extensions*, Contemporary Mathematics **25(8)** (1997), 2459-2506.

[20] O. Ore, *Theory of non-Commutative Polynomials*, Ann. Math. **34** (1933), 480-508.

[21] J. Ram, *On the Semisimplicity of Skew Polynomial Rings*, Proc. Amer. Math. Soc. **903** (1984), 347-351.

[22] L. Taelman, *Dieudonné Determinants for Skew Polynomial Rings*, arXiv: math.Ra/0304478 v1, (2003)

[23] M.G. Voskoglou, *Semprime Ideals of Skew Polynomial Rings*, Pub. Inst. Math. **47** (1990), 33-38.